Ubee DDW365
Wireless Cable Modem

Firmware Version: 8.14.2009

Subscriber User Guide
Time Warner Cable

www.ubeeinteractive.com
8085 S. Chester Street, Suite 200
Englewood, CO 80112
1.888.390.8233
Sales (email): amsales@ubeeinteractive.com
Support (email): amsupport@ubeeinteractive.com

October 2013

Notices and Copyrights

Copyright 2013 Ubee Interactive. All rights reserved. This document contains proprietary information of Ubee Interactive and is not to be disclosed or used except in accordance with applicable agreements. This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Ubee), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Ubee and the business management owner of the material.

Ubee Interactive continuously improves its products and reserves the right to make changes to the product described in this document without notice. Ubee Interactive does not assume any liability that may occur due to the use of the product described in this document.

All trademarks mentioned in this document are the property of their respective owners.

This device is Wifi Alliance Certified:

Contents

1 Introduction 1

1.1 Understanding Safety and Regulatory Information 1
1.2 Understanding Connections and Applications 3
1.3 Requesting Support 3
1.4 Checking Device Package Components 3
1.5 Understanding the Device Panels, Connections and LEDs 4
1.6 Understanding Specifications, Standards, and Firmware 6
1.7 Understanding Default Values and Logins 8

2 Installing the DDW365 9

2.1 Setting Up and Connecting the DDW365 9
2.2 Connecting Devices to the Network 10
2.3 Troubleshooting the Installation 12

3 Using the Web User Interface 13

3.1 Accessing the Web User Interface Locally 13
3.2 Logging Out of the Web Interface 14

4 Understanding the Status Menu 16

4.1 Using the Software Option 16
4.2 Using the Connection Option 18
4.3 Using the Account Option 20
4.4 Using the Diagnostics Option 21
4.5 Using the Client List Option 24
4.6 Using the User Default Option 26

5 Understanding the Basic Menu 27

5.1 Using the Setup Option 27
5.2 Using the DHCP Option 29
5.3 Using the DDNS Option 31
5.4 Using the Backup Option 32
5.5 Using the Time Option 35

6 Understanding the Advanced Menu 36

6.1 Using the Options Option 36

6.2 Using the IP Filtering Option 39
6.3 Using the MAC Filtering Option 40
6.4 Using the Port Filtering Option 41
6.5 Using the Forwarding Option 43
6.6 Using the Port Triggers Option 47
6.7 Using the Pass Through Option 49
6.8 Using the DMZ Host Option 50

7 Understanding the Firewall Menu 52

7.1 Using the Basic Option 52
7.2 Using the Local Log Option 53
7.3 Using the Remote Log Option 54

8 Understanding the Parental Control Menu 56

8.1 Using the Parental Control User Setup Option 56
8.2 Using the Basic Option 58
8.3 Using the ToD Filter Option. 60
8.4 Using the Local Log Option 61

9 Understanding the Wireless Menu 63

9.1 Using the Wireless Radio Option 63
9.2 Using the Primary Network Option 66
9.3 Using the Access Control Option 70
9.4 Using the Wi-Fi Multimedia Option 72
9.5 Using the Bridging Option 75
9.6 Deploying and Troubleshooting the Wireless Network 76

10 Glossary 80

1 Introduction

Welcome to the Ubee family of data networking products. This guide is specific to the **DDW365 Wireless Cable Modem** for subscribers of **Time Warner Cable** services. This document serves the following purposes:

- Provides instructions on how to install, connect and operate the device.
- Provides directions for accessing the Web user interface (UI) for configuration and management of the device.
- Defines all relevant device compliance standards and physical specifications.

Topics

See the following topics:

- Understanding Safety and Regulatory Information on page 1
- Understanding Connections and Applications on page 3
- Requesting Support on page 3
- Checking Device Package Components on page 3
- Understanding the Device Panels, Connections and LEDs on page 4
- Understanding Specifications, Standards, and Firmware on page 6
- Understanding Default Values and Logins on page 8

1.1 Understanding Safety and Regulatory Information

Use the following information to better understand safety and regulatory standards to install, maintain, and use the DDW365 Wireless Cable Modem.

1.1.1 Understanding Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the DDW365. Read all safety instructions in this guide before attempting to unpack, install, operate, or connect power to this product. Follow all instruction labels on the device itself. Comply with the following safety guidelines for proper operation of the device.

Follow basic safety precautions to reduce the risk of fire, electrical shock, and injury. To prevent fire or shock hazard, do not expose the unit to rain and moisture or install this product near water. Never spill any form of liquid on or into this product. Do not use liquid cleaners or aerosol cleaners on or close to this product. Clean with a soft dry cloth.

Do not insert sharp objects into the product's module openings or empty slots. Doing so can accidentally damage its parts and/or cause electric shock.

Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

Use only the power cable supplied with the device. Do not attach the power supply cable to building surfaces or floorings.

- ❑ Rest the power cable freely without any obstacles. Do not place heavy items on top of the power cable. Do not abuse, step, or walk on the cable.
- ❑ Do not place heavy objects on top of the device. Do not place the device on an unstable stand or table; the device can fall and become damaged.
- ❑ To prevent overheating, do not block the slots and openings in the module housing that provide ventilation. Do not expose this device to direct sunlight. Do not place hot devices close to this device; it may degrade it or cause damage.

1.1.2 Understanding Eco-Environmental Statements

The following eco-environmental statements apply to the DDW365.

Packaging Collection and Recovery Requirements:

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste can be established. For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, contact Ubee Interactive at www.ubeeinteractive.com.

1.1.3 Understanding Regulatory Statements

The following regulatory statements apply to the DDW365.

Industry North America Statement:

This device complies with RSS-210 of the Industry North America Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

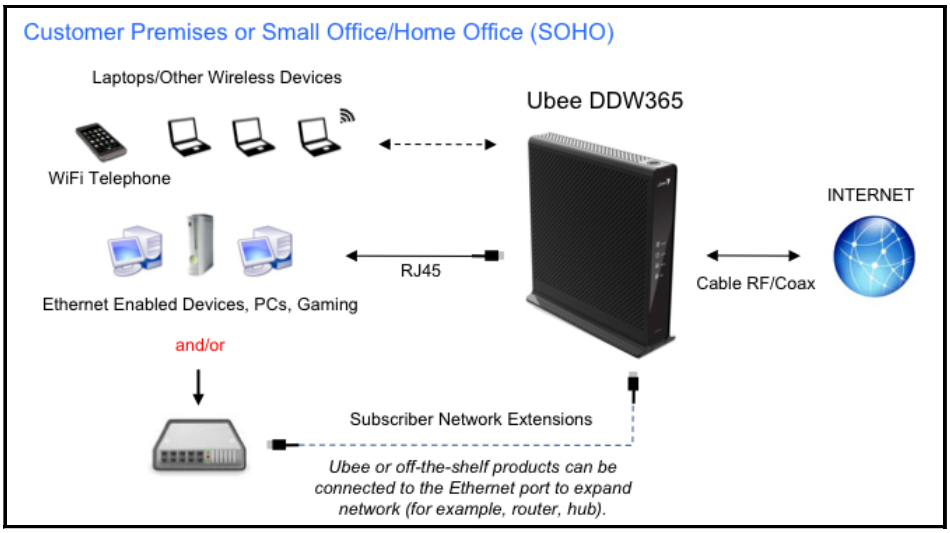
(2) This device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement:

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20cm between the radiator & your body. This device has been designed to operate with an antenna having a maximum gain of 2 dBi. This device must not be co-located with or operating in conjunction with any other antenna or transmitter.

1.2 Understanding Connections and Applications

The following diagram illustrates the general connections and applications of the DDW365.


Customer Premises or Small Office/Home Office (SOHO)
Laptops/Other Wireless Devices
Ubee DDW365
WiFi Telephone
INTERNET
RJ45
Cable RF/Coax
Ethernet Enabled Devices, PCs, Gaming
and/or
Subscriber Network Extensions
Ubee or off-the-shelf products can be connected to the Ethernet port to expand network (for example, router, hub).

1.3 Requesting Support

Subscribers must contact their service provider for direct support. Device documentation support may be available at:

http://www.ubeeinteractive.com

1.4 Checking Device Package Components

The package for the DDW365 contains the following items:

Item	Description
	1 - RJ45 Cable (Ethernet) Length ~ 6.0 ft RoHS & UL compliant *Sample image, actual appearance subject to change.*

Item	Description
	1 - Power Cable Input: 100-120V ~, 50-60Hz CE and UL Certified *Sample image, actual appearance subject to change.*

1.5 Understanding the Device Panels, Connections and LEDs

1.5.1 Understanding the Device Front and Rear Panels

The following images represent the device front and rear panels. Connection descriptions are provided in section 1.5.2., and LED descriptions are provided in section 1.5.3.

Front Panel **Rear Panel**

1.5.2 Understanding the Device Connections

The following table describes the connections on the device.

Item	Description
RESET	Restores the settings of the device, including wireless and custom gateway settings, to factory defaults. Use a pointed object to push down the recessed reset button. To power cycle the device, hold for less than 5 seconds. To reset the device to factory defaults, hold down for more than 5 seconds. After the power LED turns off, release the button.
USB	Disabled by default. If enabled by the service provider, the USB port connects to USB devices such as flash drives or hard disk drives.
ETH1 **ETH2** **ETH3** **ETH4**	Connects to Ethernet devices such as computers, gaming consoles, and/or routers/hubs using an RJ45 cable. Each ETH port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected.
CABLE	Connects to the power cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
POWER	Connects the cable to the device. Use only the power cable provided with the DDW365.
WPS	Located on top of the device, this button is used for the WiFi Protected Setup (WPS) method to connect a PIN-protected WiFi device to the cable modem. Refer to Understanding the Wireless Menu on page 63 for more information.

1.5.3 Understanding LED Behavior

The following tables summarize the behavior of the LEDs on both the front and rear panels of the DDW365.

FRONT PANEL		
LED	**Color**	**Description**
POWER	**White**	**On** – Internal power-on completed successfully. **Flashes** – Power-on failed. Note that the LED blinks briefly immediately after powering on the device. **On** – when firmware upgrade is in progress.
US/DS (upstream/ downstream)	**White**	**Flashes** – Once every second while scanning DS. Once locked on DS, flashes twice every second while registering the US. **On** – Locked to US and DS channels and registered OK. **Flashes** – When a firmware upgrade is in progress, and POWER LED and ONLINE LEDs are ON solid.

FRONT PANEL		
LED	**Color**	**Description**
ONLINE	**White**	**Flashes** – Obtaining an IP address and configuration file. **On** – Configuration completed successfully, device is connected to the network. **Off** – Network connect failed.
WiFi	**White**	**On** – WiFi is enabled. **Off** – WiFi is disabled.
WPS BUTTON (top of device)	**White**	If not used, the LED is off. When a user pushes the WPS button or triggers WPS via the device's Web UI, an LED on the top-front of the device **flashes** for 4 minutes until a PIN is entered from the wireless client that wishes to connect (for example, a laptop computer). After a WiFi client attaches successfully, the LED remains On for 5 minutes, then turns Off.

REAR PANEL		
LED	**Color**	**Description**
ETH1 **ETH2** **ETH3** **ETH4**	**Green/ Orange**	**On Green** – An Ethernet device is connected to the DDW365 at 1000 Mbps speeds (Gigabit Ethernet). **On Orange** – An Ethernet device is connected to the DDW365 at 10/100 Mbps speeds. **Flashes (in Green or Orange)** – When data is being passed between the DDW365 and the connected device. The Ethernet ports are used to connect Ethernet devices such as computers, gaming consoles, and/or routers/hubs to the DDW365 using RJ-45 cables. Each Ethernet port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected.

1.6 Understanding Specifications, Standards, and Firmware

The following list provides the features and specifications of the DDW365.

Interfaces and Standards

- ❑ Cable: F-Connector, female
- ❑ LAN: (4) 10/100/1000 Mbps RJ45 ports
- ❑ USB: (1) USB 2.0 host port
- ❑ DOCSIS 3.0 certified
- ❑ DOCSIS 1.0/1.1/2.0 certified
- ❑ CE/FCC Class B, ENERGY STAR® certified, WiFi Alliance certified

Downstream*

- ♦ Frequency Range: 88MHz ~ 1002MHz

- Modulation: 64 / 256 QAM
- Channel Bandwidth: 6 MHz
- Maximum Data Rate per Channel (up to 8 channels): DOCSIS = 30 Mbps (64 QAM), 42 Mbps (256 QAM),
- Total Max Bandwidth (8 Channels): DOCSIS = 343 (304) Mbps
- Symbol Rate: 6952 Ksps
- RF (cable) Input Power: -15 to +15dBmV (64 QAM), -15 to +15dBmV (256 QAM)
- Input Impedance: 75 Ω

Upstream*

- Frequency Range: 5MHz ~ 42MHz
- Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM
- Max Bandwidth of 4 Channels = 122.88 (108) Mbps, bandwidth per channel (up to 4 channels) = [QPSK 0.32 ~ 10.24 Mbps, 8 QAM 0.48 ~ 15.36 Mbps, 16 QAM 0.64 ~ 20.48 Mbps, 32 QAM 0.80 ~ 25.60 Mbps, 64 QAM 0.96 ~ 30.72 Mbps, 128 QAM/TCM 30.72 Mbps]
- Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- RF (cable) Output Power: TDMA/ATDMA: +8dBmV to +54dBmV (32/64 QAM). ATDMA Only: +8dBmV to +55dBmV (8/16 QAM), +8dBmV to +58dBmV (QPSK). S-CDMA: +8dBmV to +53dBmV (all modulations)

*Actual speeds vary based on factors including network configuration and speed.

Security and Network

- Supports 8 SSIDs, 802.11b/g/n compliant with link speeds up to 450 Mbps, 3 Tx and 3 Rx antennas with single radio
- DHCP Client/Server, Static IP network assignment, RIPv1/ v2, Ethernet 10/100/1000 BaseT, full-duplex auto-negotiate functionality, IPv4 and IPv6 support
- NAT Firewall, MAC/IP/port filtering, parental control, stateful packet inspection (SPI), DoS attack protection, WPS/ WPA/ WPA2/ WPA-PSK & 64/128-bit WEP encryption
- VPN pass-through and end-point support (IPSec/PPTP), TACACS or RADIUS authentication

Device Management

- Supports IEEE 802.11e Wi-Fi Multimedia (WMM) and UAPSD (power savings)
- DOCSIS, Web-Based, and XML Configuration
- Telnet/SSH remote management
- Firmware upgrade via TFTP
- Configuration backup and restore
- SNMP support
- TR-069 capable

Physical and Environmental

- Dimensions: 220mm, 8.625” (W) x 220mm, 8.625” (H) x 42mm, 1.625” (D)
- Weight: 825g (1.8 lbs.) (Contains internal PSU)

- Input: 90-120VAC, 50-60Hz
- Output: 12V 2.17A
- Operating Temperature: 0°C ~ 40°C (32°F ~ 104°F)
- Humidity: 5~90% (non-condensing)

1.7 Understanding Default Values and Logins

The DDW365 is pre-configured with the default parameters for Time Warner Cable.

Local Port Address: 192.168.100.1

Web Interface: http://192.168.100.1

Operation Mode: NAT Mode

Subnet Mask: 255.255.255.0

Wireless Defaults:

- Primary SSID (subscriber-managed) = “DDW365” plus the last 2 characters of the MAC address with the letters entered in UPPER case.

  Example: **DDW3658C**

  - If the subscriber changes the SSID, the device does not revert to this default SSID when the device is reset, except when a manual reset is performed through the Web UI.
  - The MAC address can be found on the device label or it can be found by opening an Internet browser window to the device. Refer to Using the Software Option on page 16 for instructions.
- Encryption Method = **WPA2-PSK** with **AES** encryption
- WPA Pre-shared Key = Unique key for each device. Also called the network key. The pre-shared key for the DDW365 is “DDW365” plus the last 6 characters (3 octets) of the modem’s MAC address, with letters entered in UPPER case. Refer to Using the Primary Network Option on page 66 for more information.

  Example: **DDW3654B488C**
- WPS PIN = The WPS PIN is a randomly-generated eight digit number found on the Wireless Primary Network screen. Refer to Using the Primary Network Option on page 66.
- Device Name: **UbeeAP**

Login Default Values

- Standard User/Subscriber Web Interface Login

  Username: **user**

  Password: **user**

2 Installing the DDW365

Use the information in this chapter to set up and connect the DDW365, connect additional devices, and troubleshoot the installation.

Topics

See the following topics:

- Setting Up and Connecting the DDW365 on page 9
- Connecting Devices to the Network on page 10
- Troubleshooting the Installation on page 12

2.1 Setting Up and Connecting the DDW365

Use the following instructions to set up and connect the DDW365. When the device is set up and connected, refer to Accessing the Web User Interface Locally on page 13 to configure the device.

Important: Subscribers will need to contact their service provider to enable Internet access and wireless networking.

Typically, the service provider initially configures and connects the device. The installation steps are provided below if you wish to confirm the setup, or add devices to your network. Refer to Connecting Devices to the Network on page 10.

Steps

To set up the device:

1. Remove the contents from the device packaging.
2. Place the DDW365 in a central location to connect to other devices, such as PCs or gaming consoles.
   - Place the DDW365 and wireless clients in open areas far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals. A wireless signal can become weaker after it has passed through metal, concrete, brick, walls, or floors.
   - Place the device in a location that has an operating temperature of 0˚ C to 40˚ C (32˚ F to 104˚ F). Refer to Understanding LED Behavior on page 5 for more safety information.
3. Power on your PC. The PC must have an Ethernet network adapter or Ethernet port and an Internet browser installed, such as Internet Explorer. The following browsers are supported:
   - For Windows 2000, XP, Vista, Windows 7, Windows 8, Google Chrome, Firefox 1.07 and higher, Internet Explorer v7 and above.

- For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.

4. Connect the power cable included in the product package to the back of the DDW365 and plug the other end into the power outlet.
5. Connect the network cable included in the product package to your computer's Ethernet port. Connect the other end to the ETH1, ETH2, ETH3, or ETH4 port on the DDW365.
6. Connect a coaxial cable from the **CABLE** connector on the back of the device to the cable wall outlet, or to a cable splitter connected to the wall outlet.
7. Validate the network connection using the device LEDs to confirm operations.
   - The WiFi LED must be flashing or solidly lit.
   - The PWR, US/DS, and ONLINE LEDs are solidly lit.

   Refer to Understanding LED Behavior on page 5 for more information.

2.2Connecting Devices to the Network

Use the instructions below to connect network devices and validate device functionality.

Topics

See the following topics:

- Connecting an Ethernet Device on page 10
- Connecting a Wireless Device on page 11

2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the DDW365.

Steps

To connect another Ethernet device to the network:

1. Connect the Ethernet cable from the Ethernet device (for example, a PC or gaming console) to an open Ethernet port on the back of the DDW365.
2. Use the device LEDs to confirm operations. Refer to Understanding LED Behavior on page 5 for more information.
3. Open a Web browser and go to any Web site to validate network/Internet connectivity (for example, http://www.wikipedia.org).
4. If the connected device is a gaming console, perform any online task supported by the console (for example, log into the gaming server, play an online game, download content).

Note

Refer to Troubleshooting the Installation on page 12 for troubleshooting information.

2.2.2 Connecting a Wireless Device

Use the following steps to connect a wireless device to the DDW365 (for example, a laptop computer).

Default values are shown in the steps below. Some regions may change default values using the DDW365 or XML configuration file.

Steps

To connect a wireless device to the DDW365:

1. Access the wireless networking menu on your wireless device. On a Windows computer, for example, double-click the **Wireless Network Connection** icon in the system tray (lower-right side of the Windows desktop).
2. Click **View Wireless Networks**. The device is shipped with a default SSID. The SSID is the name of the wireless network broadcast from the device so that wireless clients can connect to it.
   - Double-click your **SSID** in the wireless networks window. The default SSID (subscriber-managed) = “DDW365” plus the last 2 characters of the MAC address with the letters entered in UPPER case.

     Example: **DDW3658C**

   Notes: You can find the MAC address on the device label or by opening an Internet browser window to the device. Refer to Using the Software Option on page 16 for instructions. If the subscriber changes the SSID, the device does not revert to this default SSID upon any reset of the device, except in the case of a manual reset using the device’s Web UI. See Using the Account Option on page 20.

   When prompted, enter the network key, also called the pre-shared key. This is a unique key for each device. The pre-shared key for the DDW365 is “DDW365” plus the last 6 characters (3 octets) of the device’s MAC address, with letters entered in UPPER case. Refer to Using the Primary Network Option on page 66.

   Example pre-shared key: DDW3654B488C

   - If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number found on the Wireless Primary Network screen. Refer to Using the Primary Network Option on page 66.
   - **WPA-WPA2 + AES** is the default encryption method.

3. Confirm connectivity by opening a Web browser and going to any Web site (for example, http://www.wikipedia.org) or access the Web interface for the DDW365.

Note

The Web interface allows you to customize the configurations and capabilities for the device. For a full explanation of all Web interface functions, refer to Using the Web User Interface on page 13.

If you have wireless issues or questions, refer to Deploying and Troubleshooting the Wireless Network on page 76.

2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

- **None of the LEDs are on when I power on the DDW365.**
  - Check the connection between the power outlet and the power cord. Verify the power outlet is energized and the power cord is connected to the power outlet.
  - Check the connection between the power cord and the device. Power off the DDW365 and wait for 5 seconds and power it on the again. If the problem still exists, there may be a hardware problem.
- **The ETH1, ETH2, ETH3, or ETH4 LEDs on the back of the DDW365 are not lit where Ethernet cables are connected.**
  - Restart the computer so that it can re-establish a connection with the device.
  - Check for a resource conflict (Windows users only):
    1. Right-click **My Computer** on your desktop and choose **Properties**.
    2. Choose the **Device Manager** tab and look for a yellow exclamation point or red **X** over the network interface card (NIC) in the Network Adapters field. If you see either one, you may have an interrupt request (IRQ) conflict. Refer to the manufacturer's documentation or ask your service provider for further assistance.
  - Verify that TCP/IP is the default protocol for your network interface card.
  - Power cycle the DDW365 by removing the power cord from the electrical outlet and plugging it back in. Wait for the device to re-establish communications with your cable service provider.
- **Check General Connectivity Issues:**
  - If your PC is connected to a hub or gateway, connect the PC directly into an Ethernet port on the DDW365.
  - If you are using a cable splitter, remove the splitter and connect the device directly to the cable wall outlet. Wait for the device to re-establish communications with the cable service provider.
  - Try a different cable. The Ethernet cable may be damaged.
- If none of these suggestions work, contact your service provider's tier II support for further assistance.

3 Using the Web User Interface

The Web user interface (UI) for the DDW365 is easy to use and allows you to view and configure settings for your device. You can validate the installation by accessing the Web user interface on the device.

Topics

See the following topics:

- Accessing the Web User Interface Locally on page 13
- Logging Out of the Web Interface on page 14

3.1 Accessing the Web User Interface Locally

Access the Web user interface for the DDW365 from a Web browser, such as Internet Explorer on a Windows computer.

Default values are shown in the steps below.

Steps

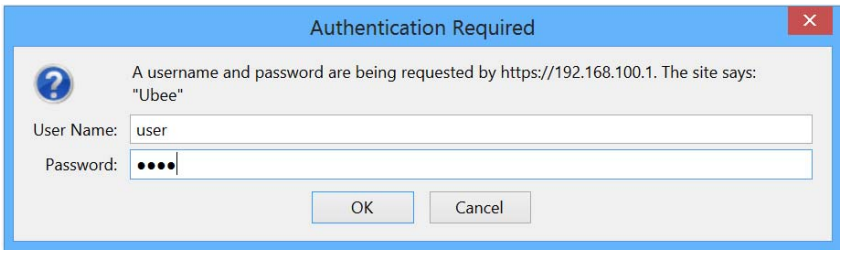
To access the Web user interface:

1. Launch an Internet browser, such as Internet Explorer, from your computer.
2. Enter the following IP address in the address bar of the browser window and press the Enter key.

   http://192.168.100.1

3. Enter the username and password in the authentication dialog box.
   - **Standard User (subscriber) Web Interface Login**:

     Username: **user**
     Password: **user**



4. Click **OK**. The Status>Software screen (shown below) displays software information

about the DDW365.

3.2 Logging Out of the Web Interface

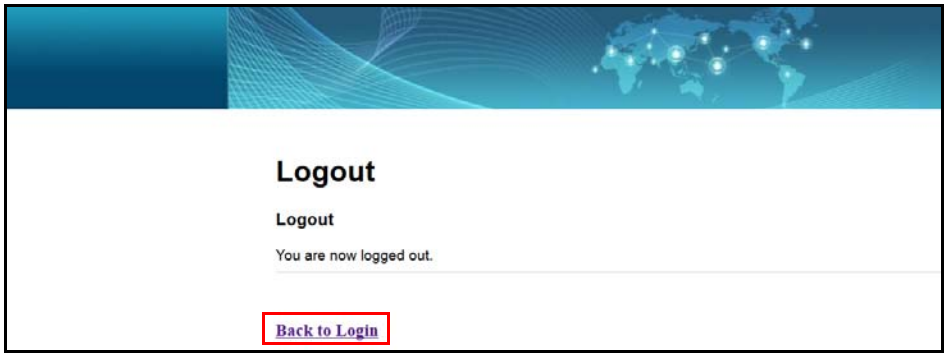
Log out when finished using the Web user interface.

Steps

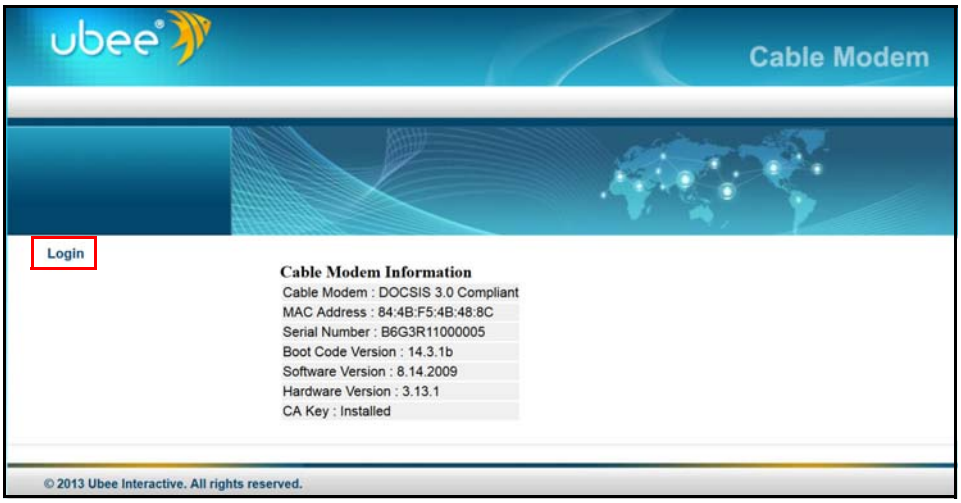
To log out of the user interface:

1. Click **Logout** from the main menu.

The logout screen is displayed.



2. To begin a new user interface session, click **Back to Login.** The Cable Modem Information screen is displayed. Click **Login** to access the login screen.



4 Understanding the Status Menu

The **Status** menu of the Web user interface allows you to access information about the DDW365, such as software, connection (downstream and upstream), diagnostics, and event log.

Topics

See the following topics:

- Using the Software Option on page 16
- Using the Connection Option on page 18
- Using the Account Option on page 20
- Using the Diagnostics Option on page 21
- Using the Client List Option on page 24
- Using the User Default Option on page 26

Steps

To access status options:

1. Access the Web user interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click **Status** from the main menu.

4.1 Using the Software Option

The **Software** option displays the device's internal software and hardware configuration.

Steps

To view software information:

1. Click **Status** from the main menu.
2. Click **Software** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
Information	
Standard Specification Compliant	Defines the current DOCSIS standard supported by of device.
Hardware Version	Defines the internal version number that identifies the hardware design.
Software Version	Defines the firmware version of the device.
Cable Modem MAC Address	Defines the unique media access control (MAC) hardware address of the DDW365.
Cable Modem Serial Number	Defines the unique manufacturer serial number of the device.
CM certificate	Indicates if the cable modem certificate is installed.
Status	
System Up Time	Displays how long the device has been connected.
Network Access	Defines if network access is enabled. When enabled, the user is allowed to access the network.
Cable Modem IP Address	Displays the IP address for the cable modem.

4.2 Using the Connection Option

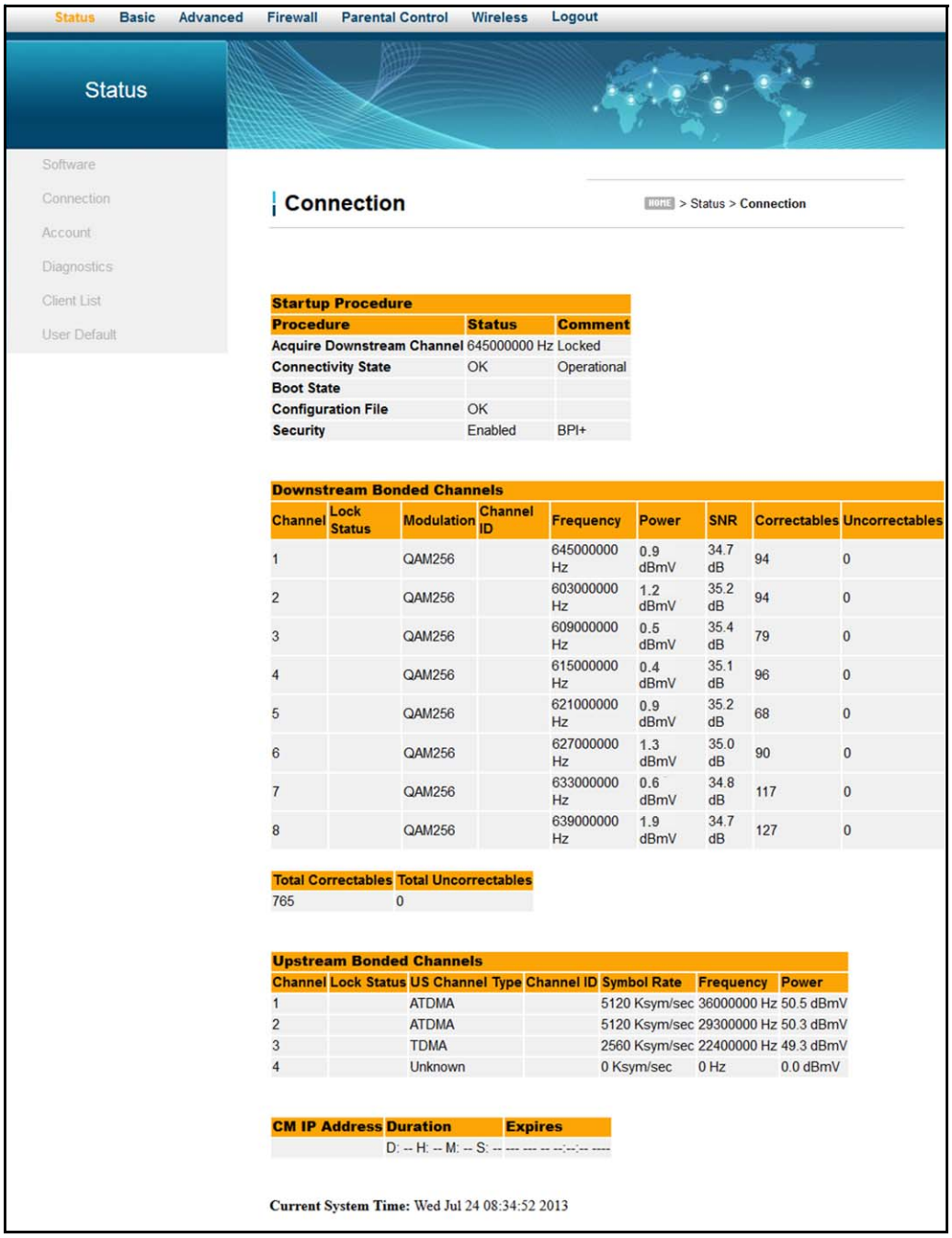
The **Connection** screen displays information about the device's connection status and downstream and upstream channel bonding statistics.

- **Downstream** displays detailed information on the network traffic from the service provider **to** the local computer (downstream channels).
- **Upstream** displays detailed information on the network traffic **from** the computer to the remote destination (upstream channels).

Steps

To view connection information:

1. Click **Status** from the main menu.
2. Click **Connection** from the left side menu. Field descriptions are listed below the screen example.


Status Basic Advanced Firewall Parental Control Wireless Logout
Status
Software
Connection
Account
Diagnostics
Client List
User Default
Connection
HOME > Status > Connection
Startup Procedure
Procedure Status Comment
Acquire Downstream Channel 645000000 Hz Locked
Connectivity State OK Operational
Boot State
Configuration File OK
Security Enabled BPI+
Downstream Bonded Channels
Channel Lock Status Modulation Channel ID Frequency Power SNR Correctables Uncorrectables
1 QAM256 645000000 Hz 0.9 dBmV 34.7 dB 94 0
2 QAM256 603000000 Hz 1.2 dBmV 35.2 dB 94 0
3 QAM256 609000000 Hz 0.5 dBmV 35.4 dB 79 0
4 QAM256 615000000 Hz 0.4 dBmV 35.1 dB 96 0
5 QAM256 621000000 Hz 0.9 dBmV 35.2 dB 68 0
6 QAM256 627000000 Hz 1.3 dBmV 35.0 dB 90 0
7 QAM256 633000000 Hz 0.6 dBmV 34.8 dB 117 0
8 QAM256 639000000 Hz 1.9 dBmV 34.7 dB 127 0
Total Correctables Total Uncorrectables
765 0
Upstream Bonded Channels
Channel Lock Status US Channel Type Channel ID Symbol Rate Frequency Power
1 ATDMA 5120 Ksym/sec 36000000 Hz 50.5 dBmV
2 ATDMA 5120 Ksym/sec 29300000 Hz 50.3 dBmV
3 TDMA 2560 Ksym/sec 22400000 Hz 49.3 dBmV
4 Unknown 0 Ksym/sec 0 Hz 0.0 dBmV
CM IP Address Duration Expires
D: -- H: -- M: -- S: -- --- --- -- --:--:-- ----
Current System Time: Wed Jul 24 08:34:52 2013

Label	Description
Startup Procedure (Procedure, Status, Comment)	
Acquire Downstream Channel	Displays the Downstream channel status and if the device has locked to a channel.
Connectivity State	Displays connection status and if the DDW365 is operational.
Boot State	Displays the status on boot up and if the device is operational.

Label	Description
Configuration File	Provides the status and file name of the configuration file currently used by the DDW365.
Security	Displays the status of the security settings: enabled/disabled.
Downstream Bonded Channels	
Channel	Numbers the downstream channels.
Lock Status	Displays if the device has locked successfully to a downstream channel.
Modulation	Displays the modulation method required for the downstream channel to lock on to by the device. This method is determined by the service provider.
Channel ID	Displays the downstream channel ID.
Frequency	Displays the downstream channel frequency on which the device is scanning.
Power	Displays the receiver power level in decibel millivolts (dBmV) after ranging process.
SNR	Displays the signal-to-noise ratio, the desired signal level to the background noise level.
Correctables	Displays the quantity of codewords which are correctable.
Uncorrectables	Displays the quantity of codewords which are not correctable.
Upstream Bonded Channels	
Channel	Numbers the upstream channels.
Lock Status	Displays if the DDW365 has locked successfully to an upstream channel.
US Channel Type	Displays the channel type.
Channel ID	Displays the current upstream channel ID.
Symbol Rate	Displays the symbol rate in 1000 symbols per second.
Frequency	Displays the current upstream frequency in hertz.
Power	Displays the current upstream transmit power in decibel millivolts (dBmV).
CM IP Address	Displays the DDW365's IP address.
Duration	Displays the time the device has been active.
Expires	Displays when the cable modem's certificate expires.

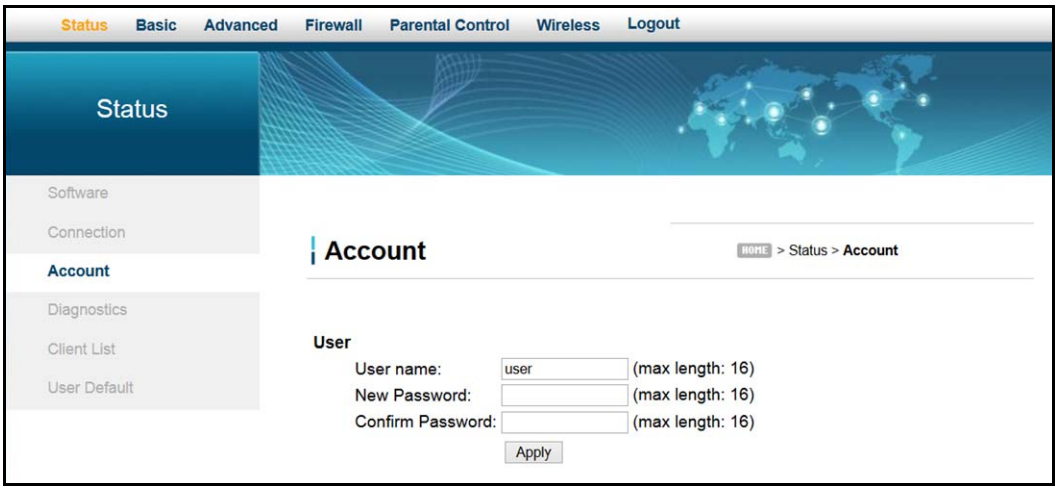
4.3 Using the Account Option

Use the **Account** option to change the Admin password and the User username and passwords.

Steps

To reset the DDW365's usernames and passwords:

1. Click **Status** from the main menu.
2. Click **Account** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
User	
New Username	Enter the new User username.
New Password	Enter the new User password.
Confirm Password	Confirm the new User password.
Apply	Saves the changes.

4.4 Using the Diagnostics Option

Use the **Diagnostics** option to test network connectivity. Two utilities are available: Ping and Traceroute.

Topics

See the following topics:

- Using the Ping Option on page 21
- Using the Traceroute Option on page 23

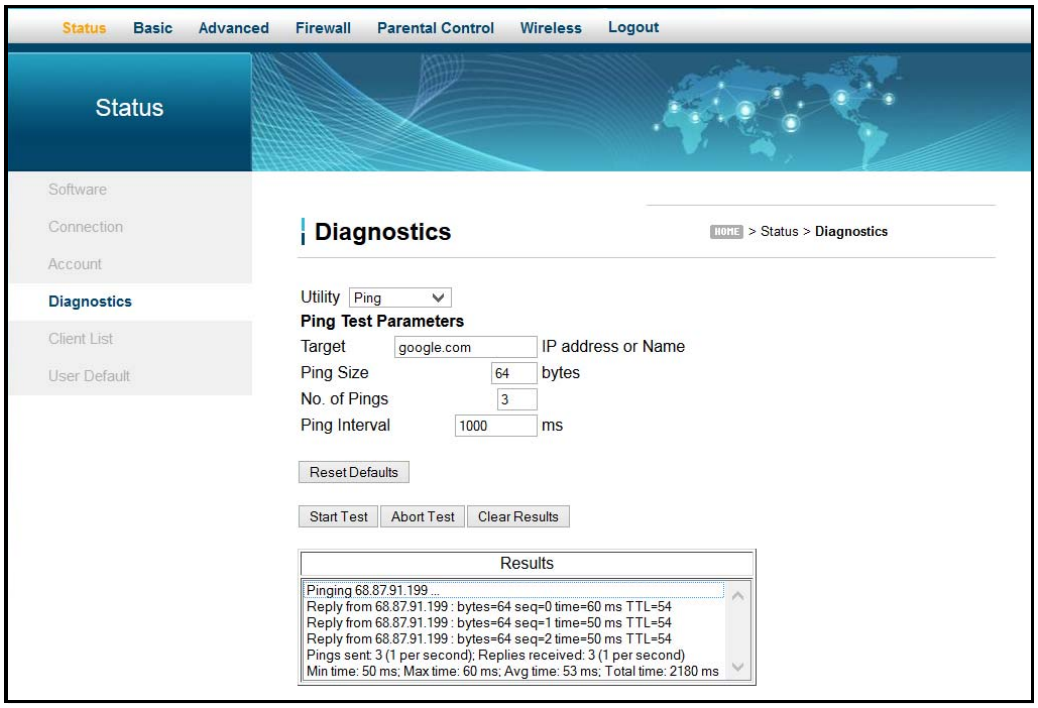
4.4.1 Using the Ping Option

Use the **Ping** utility to test network connectivity between devices by sending a test message to a specific device. You can also confirm the size of data sent is the same as the size of data received.

Steps

To test connectivity between devices:

1. Click **Status** from main menu.
1. Click **Diagnostics** from the left side menu.
2. Choose **Ping** from the Utility drop-down menu.
3. Enter new parameter values or accept the default values.
4. Click **Start Test**. Field descriptions are listed below the screen example.



Label	Description
Utility	Provides a drop-down menu to choose Ping or Traceroute.
Ping Test Parameters	
Target	Defines the IP address to which you want to send a ping.
Ping Size	Defines the packet size (bytes of data) to send for the ping operation. Default is 64.
No. of Pings	Defines the number of ping commands to send to the ping target. Default is 3 pings.

Label	Description
Ping Interval	Defines the interval between ping operations in milliseconds.
Start Test **Abort Test** **Clear Results**	Defines what action to take. ♦ Start Test begins the ping. ♦ Abort Test stops the ping. ♦ Clear Results deletes previous test results in the Results table.
Results	Displays the results of the ping test.

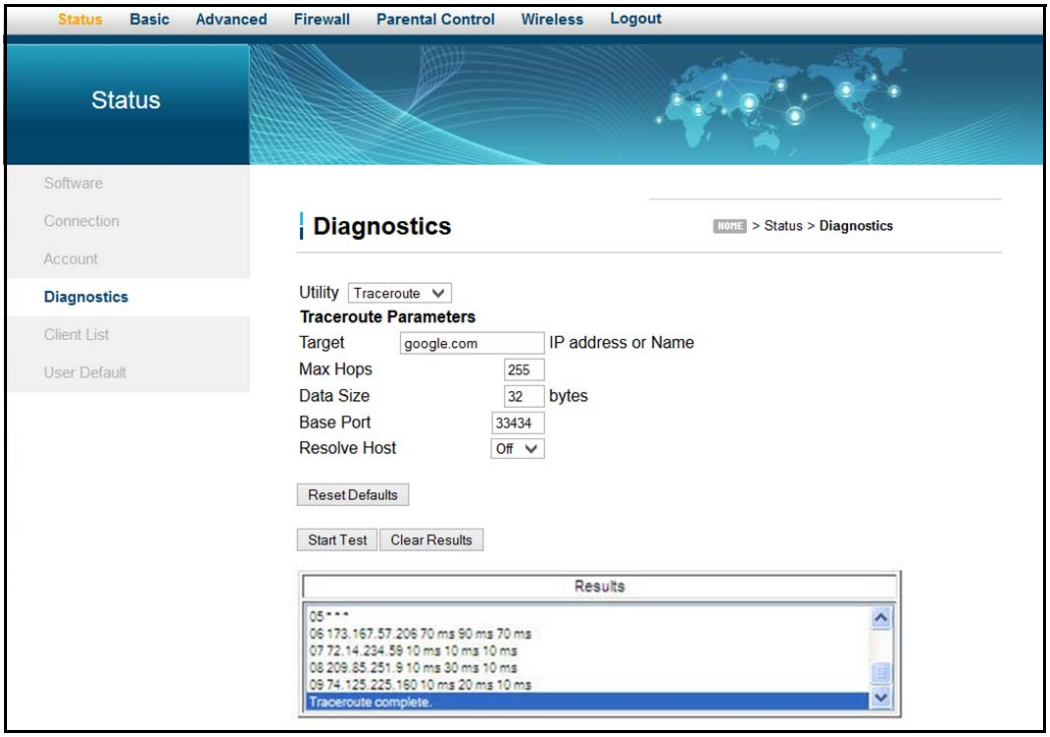
4.4.2 Using the Traceroute Option

The **Traceroute** utility determines the IP addresses of hosts in the network path. By checking the Resolve Host names box, Traceroute tries to find which name matches the address. Some hosts have no names, and might still be shown as IP addresses, even if this option is active.

Steps

To trace host IP addresses along a route:

1. Click **Status** from main menu.
2. Click **Diagnostics** from the left side menu.
3. Choose **Traceroute** from the Utility drop-down menu.
4. Enter new parameter values or accept the default values.
5. Click **Start Test**. Field descriptions are listed below the screen example.



Utility	Provides a drop-down menu to choose Ping or Traceroute.
Traceroute Parameters	
Target	Defines the specific IP address or domain (for example, google.com) to which you want to trace a route.
Max Hops	Defines the maximum number of hops. Hops are the number of routers the traceroute traverses. Default is 30.
Data Size	Defines the data size to send for the traceroute operation. The default is 64.
Base Port	Defines the destination port number. Default is 33434.
Resolve Host	Enable (on) or disables (off) this option. When checked, traceroute tries to find the name that matches the IP address. Default is Off.
Start Test/Clear Results	Defines what you want to do: ♦ Start Test begins the traceroute. ♦ Clear Results deletes previous test results in the Results table.
Results	Displays the results of the trace.

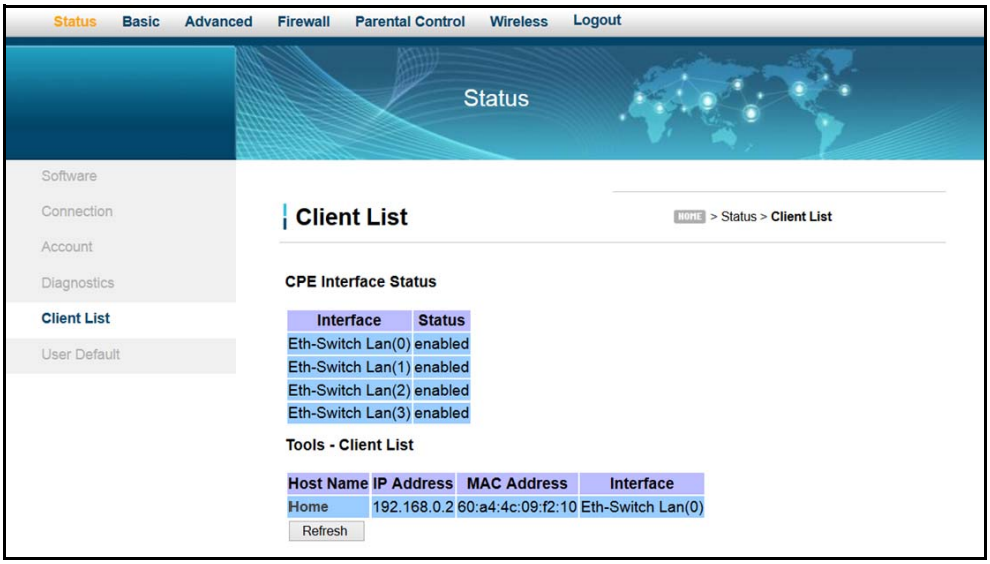
4.5 Using the Client List Option

The **Client List** screen displays computers and devices connected to the DDW365.

Steps

To view a list of connected devices:

1. Click **Status** from the main menu.
2. Click **Client List** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
CPE Interface Status	
Interface	Displays the interface.
Status	Displays whether the CPE Interface is enabled or disabled.
Tools Client List	
Host Name	Displays the host name of the DHCP client connected to the DDW365.
IP Address	Displays the IP address of the DHCP client connected to the DDW365.
MAC Address	Displays the MAC address of the DHCP client connected to the DDW365.
Interface	Displays the method of how clients are connected to the device (for example, Ethernet LAN, Wireless).
Refresh	Refreshes the client list. This may be useful when testing network connectivity between connecting clients and the DDW365.

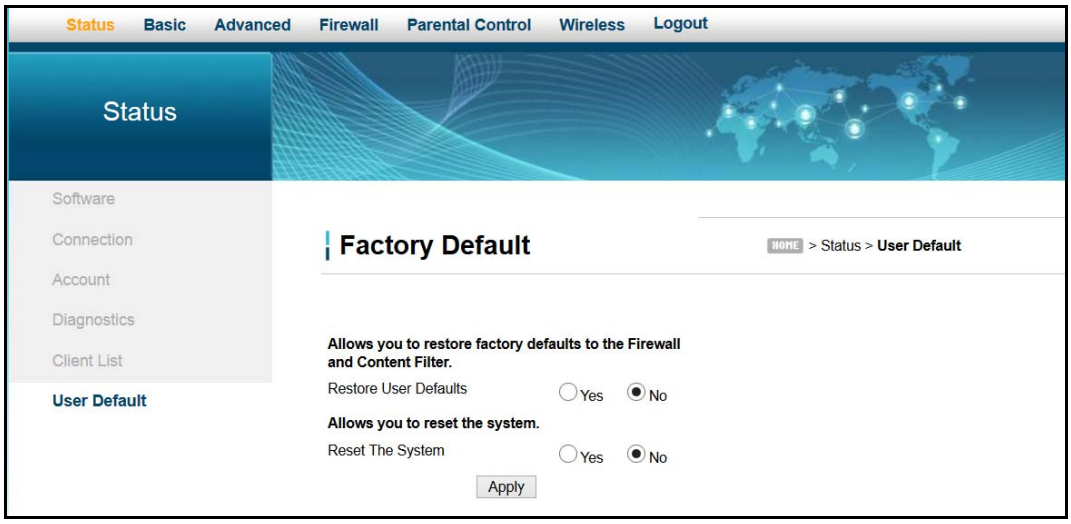
4.6 Using the User Default Option

The **User Default** option allows you to restore factory defaults to the Firewall and Parental Control settings. All other networking settings are not cleared and reset (for example, wireless settings).

Steps

To restore user defaults:

1. Click **Status** from the main menu.
2. Click **User Default** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Restore User Defaults	Restores settings to factory defaults. Select Yes, then Apply, to restore the device to the default Firewall and Parental Control Content Filter settings. This operation does not require a reset (power cycle) of the device.
Reset The System	Resets the system. Select Yes to power cycle the device. When you select Apply, you will be notified that the device has been reset. Click RELOAD. The Login screen will then appear.
Apply	Applies the options selected on this screen.

5 Understanding the Basic Menu

Basic gateway options provide the majority of configuration for the device including WAN IP addresses, LAN IP addresses, and DHCP. Advanced gateway options provide settings like MAC filtering and port forwarding.

Topics

See the following topics:

- Using the Setup Option on page 27
- Using the DHCP Option on page 29
- Using the DDNS Option on page 31
- Using the Backup Option on page 32
- Using the Time Option on page 35

Steps

To access the basic menu:

1. Access the Web user interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click **Basic** from the main menu.

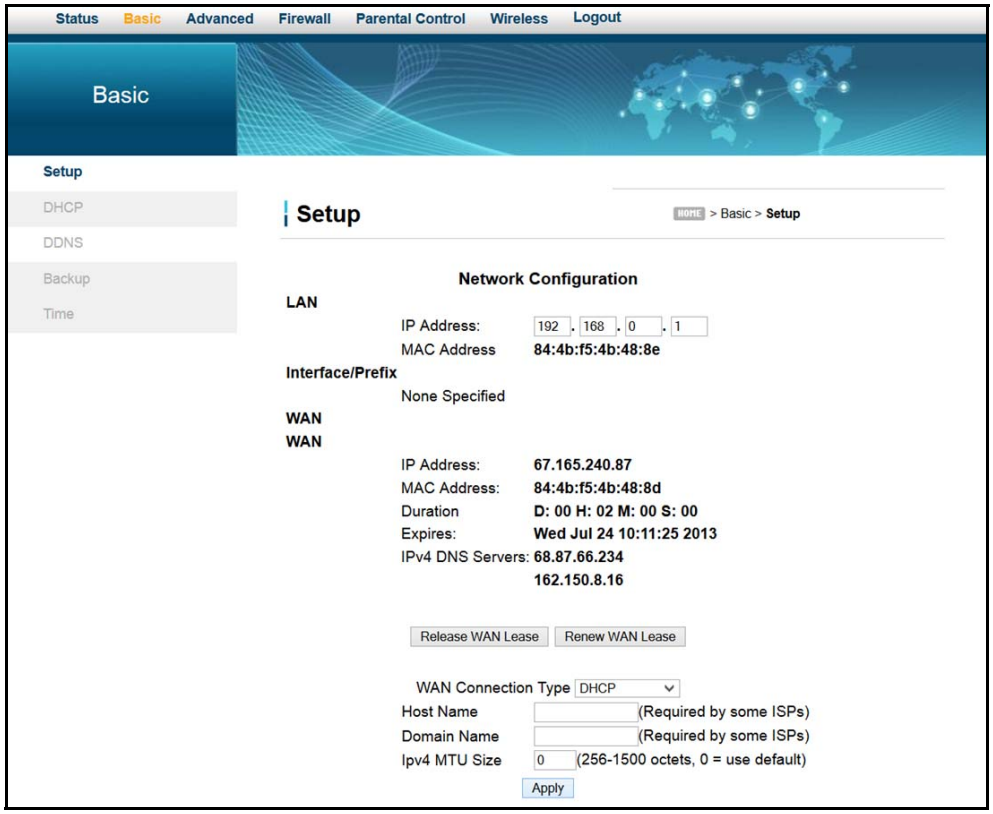
5.1 Using the Setup Option

Use the **Setup** option to configure common gateway parameters.

Steps

To configure setup options:

1. Click **Basic** from the main menu.
2. Click **Setup** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
LAN	
IP Address	Defines the local IP address, which is the default gateway address for all wired LAN hosts that connect to the DDW365.
MAC Address	Displays the LAN interface's hardware address.
Interface/Prefix	
None Specified	Indicates no interface or prefix has been specified.
WAN	
IP Address	Displays the current WAN public IP address obtained from the service provider.
MAC Address	Displays the WAN interface's hardware address.
Duration	Displays the accumulated time since successfully acquiring a WAN public IP address.
Expires	Displays the remaining time before the WAN IP address expires, if applicable.
IPv4 DNS Servers	Lists the DNS servers available on the network.
Release WAN Lease	Releases the WAN public IP address when clicked.
Renew WAN Lease	Renews the WAN IP address when clicked.

Label	Description
WAN Connection Type	Selects the WAN connection type. For each type, different data entry is required, as explained below: ♦ DHCP: The WAN interface is set to a DHCP client, and the IP address is assigned by the service provider's DHCP server. ♦ Static IP: For Static IP, you must manually enter the IP address for the WAN interface. ♦ PPTP (dhcp): For Point to Point Tunneling Protocol (PPTP), you must enter a username, password, and the PPTP server's IP address. ♦ PPTP (static): ♦ L2TP (dhcp): ♦ L2TP (static):
Host Name	Defines the host name for the router. This may be required by some service providers.
Domain Name	Defines the domain name for the router. This may be required by some service providers.
IPv4 MTU Size	Defines the maximum transmission unit (MTU) size. MTU defines the largest size of the packet or frame that the device can transfer (256-1500). If this is not given by your service provider, use 0 for the default.
Apply	Saves changes.

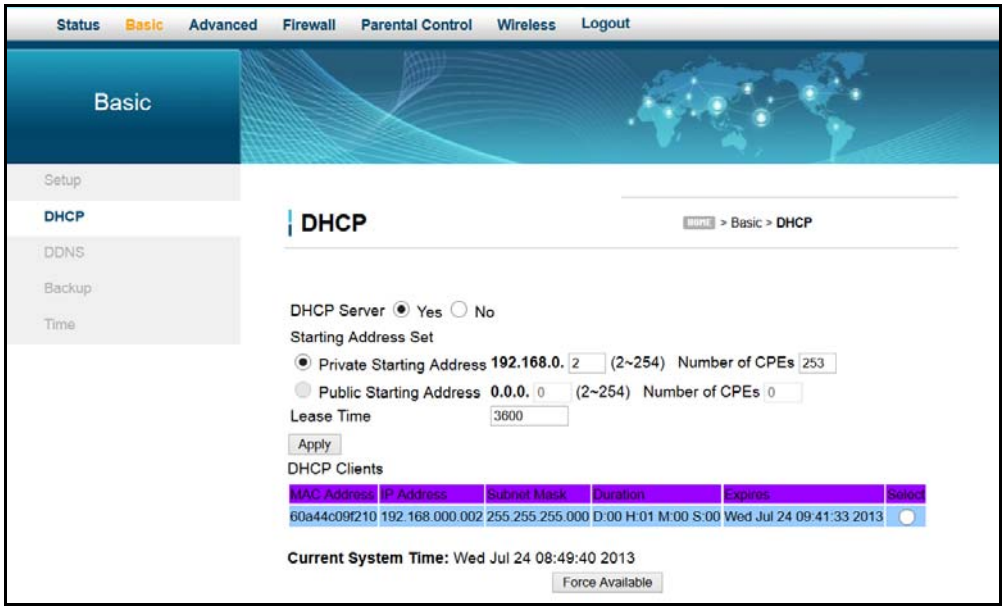
5.2 Using the DHCP Option

Use the **DHCP** option to configure dynamic host configuration protocol-specific behavior on the device.

Steps

To configure DHCP settings:

1. Click **Basic** from the main menu.
2. Click **DHCP** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
DHCP Server	Enables (Yes) or disables (No) DHCP on the device. If No is selected, all the static DHCP rules in this screen are ignored.
Starting Address Set	
Private Starting Address	Defines the starting private IP address for the pool of IP addresses that can be used by connecting clients. Private addresses are translated to public IPs to be used on the network.
Public Starting Address	Defines the starting public IP address. Public addresses can be recognized on the network.
Number of CPEs	Defines the maximum number of customer premises equipment devices (CPE) that can connect to the network through the DDW365.
Lease Time	Defines the DHCP lease time duration in minutes between 1 and 71582788. A DHCP user's PC gets an IP address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be issued a new unused IP address. **Note:** The default DHCP lease time is 3600 seconds and should be changed to **86400** seconds (24 hours). This helps resolve connectivity issues with some iMAC and Windows 7 devices that turn off the network interface when they go into standby mode. This results in slow Web browsing until the device gets a new IP address via DHCP.
Apply	Saves changes.

Label	Description
DHCP Clients	Lists all DHCP clients currently connected to the device, either via an Ethernet connection, or via a wireless connection. Each client is listed with the following information: ♦ MAC Address / IP Address / Subnet Mask ♦ Duration: Duration displays the accumulated time since the client acquired the IP address. ♦ Expires: Expires is the time until the IP expires and must be recycled. If the IP address is reserved to a certain host, it shows STATIC IP ADDRESS. ♦ Select: Reserves the current private IP address to be assigned to this host statically when selected.
Current System Time	Displays the current system time.
Force Available	Activates a selected rule in the DHCP Clients list and assigns IP addresses. Note: The Select button must be activated in the DHCP list.

5.3 Using the DDNS Option

Use the dynamic domain name system (DDNS) to assign a changing IP address to a constant pre-defined host name. The host can then be contacted by other hosts on the Internet, even if its IP address changes.

The DDNS service for the DDW365 is provided through a third-party and can be purchased from Dynamic Network Services Inc. at www.dynDNS.com.

Steps

To use the DDNS option:

1. Click **Basic** from the main menu.
2. Click **DDNS** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
DDNS Service	Enables or disables the DDNS service. When enabled, this service is available from www.dynDNS.org.
User Name	Defines the user name for the DDNS account.
Password	Defines the password for the DDNS account.
Host Name	Defines the host name for the DDNS account.
IP Address	Displays the IP address for the DDNS account.
Status	Displays if the DDNS service is enabled or disabled.
Apply	Saves changes.

5.4 Using the Backup Option

The Backup option lets you backup your gateway configuration or restore the DDW365 to a previously saved configuration.

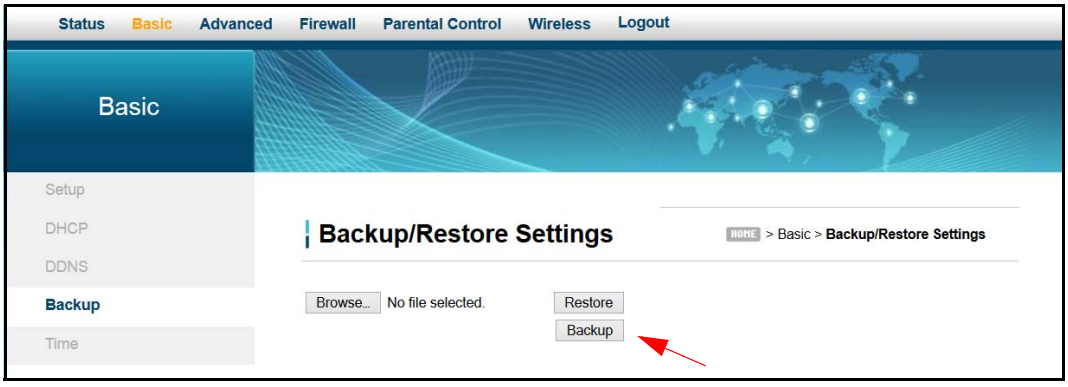
Steps

To use the backup option:

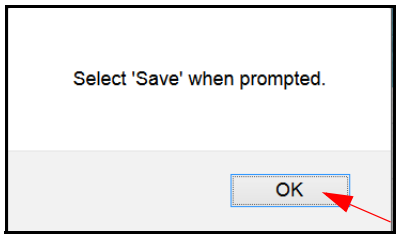
1. Click **Basic** from the main menu.
2. Click **Backup** from the left side menu.

5.4.1 Backing Up the Current Configuration

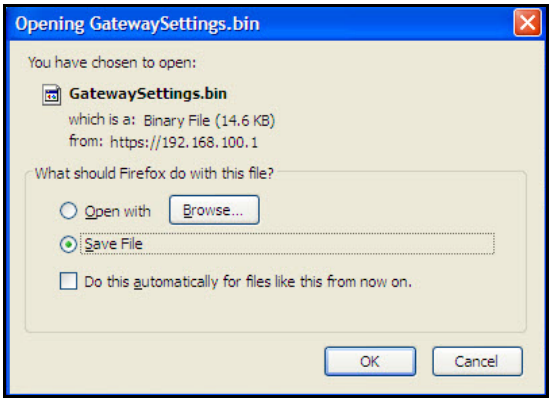
To backup and save the current modem configuration, click the **Backup** button.



A pop-up window appears instructing you to select '**Save**' when prompted. Click '**OK**'.



The following window appears, giving you the option to save the file. Click the '**Save File**' option and click '**OK**'.

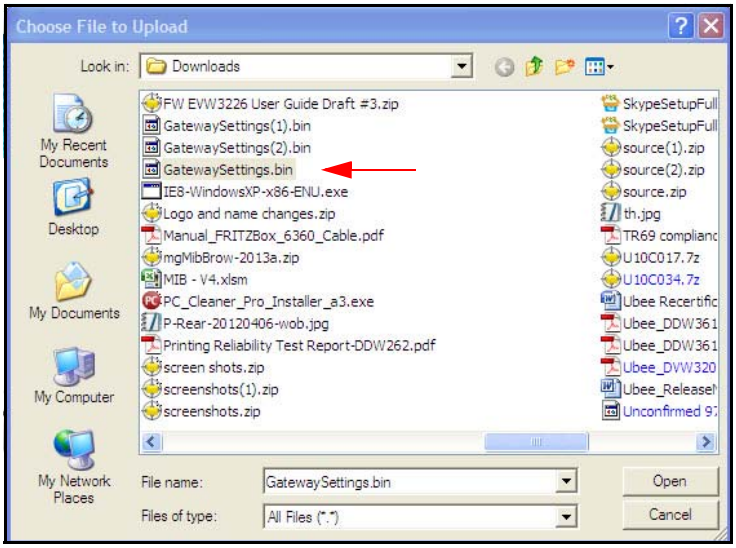


The file will be saved to your Downloads folder as a binary file (.bin) titled 'GatewaySettings.bin.'

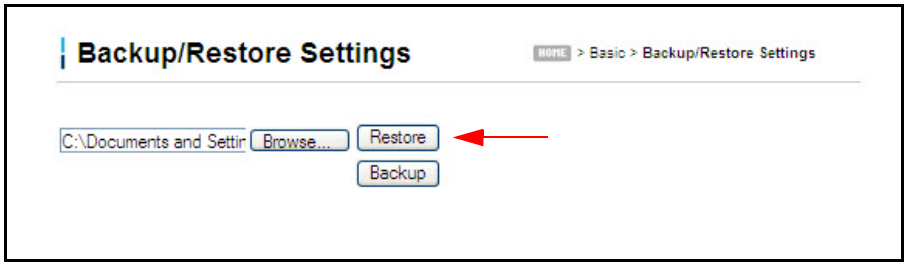
5.4.2 Restoring the DDW365 to a Previously Saved Configuration

To restore the device to a previously saved configuration, click the **Browse** button.

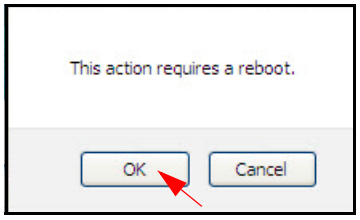
The File Upload dialog box appears and allows you to select the previously saved backup file. Highlight the file and click '**Open**'.



The location for the backed up file appears in the box to the left of the Browse button. Click the **Restore** button.



You are advised that you will be required to reboot the device. Click '**OK**'.



You are then notified that the device has been reset. Click '**RELOAD**'.

You are then presented with the login screen. Enter the Username and Password to return to the User Interface.

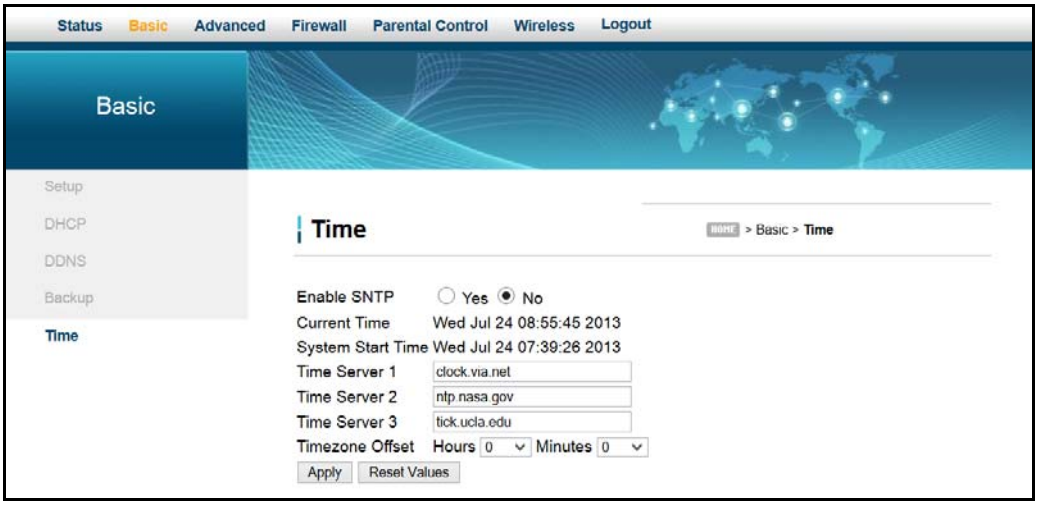
5.5 Using the Time Option

The **Time** option allows you to configure the system time obtained from the network servers via Simple Network Time Protocol (SNTP). SNTP is a protocol for synchronizing the clocks of computing devices over networks. The device must be reset for changes to take effect.

Steps

To configure system time:

1. Click **Basic** from the main menu.
2. Click **Time** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Enable SNTP	Enables (Yes) or disables (No) the SNTP feature.
Current Time	Displays the current system time.
System Start Time	Displays the time the system was started.
Time Server 1	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.
Time Server 2	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.
Time Server 3	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.
Time Zone Offset	Defines the time zone offset in hours and minutes from Greenwich Mean Time. For example: 8 hours means GMT +8, -1 hour means GMT -1.
Apply	Saves changes.
Reset Values	Resets the screen to factory defaults when clicked.

6 Understanding the Advanced Menu

Advanced options provide settings to configure your DDW365, such as MAC filtering and port forwarding.

Topics

See the following topics:

- Using the Options Option on page 36
- Using the IP Filtering Option on page 39
- Using the MAC Filtering Option on page 40
- Using the Port Filtering Option on page 41
- Using the Forwarding Option on page 43
- Using the Port Triggers Option on page 47
- Using the Pass Through Option on page 49
- Using the DMZ Host Option on page 50

Steps

To access the advanced menu:

1. Access the Web User Interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click **Advanced** from the main menu.

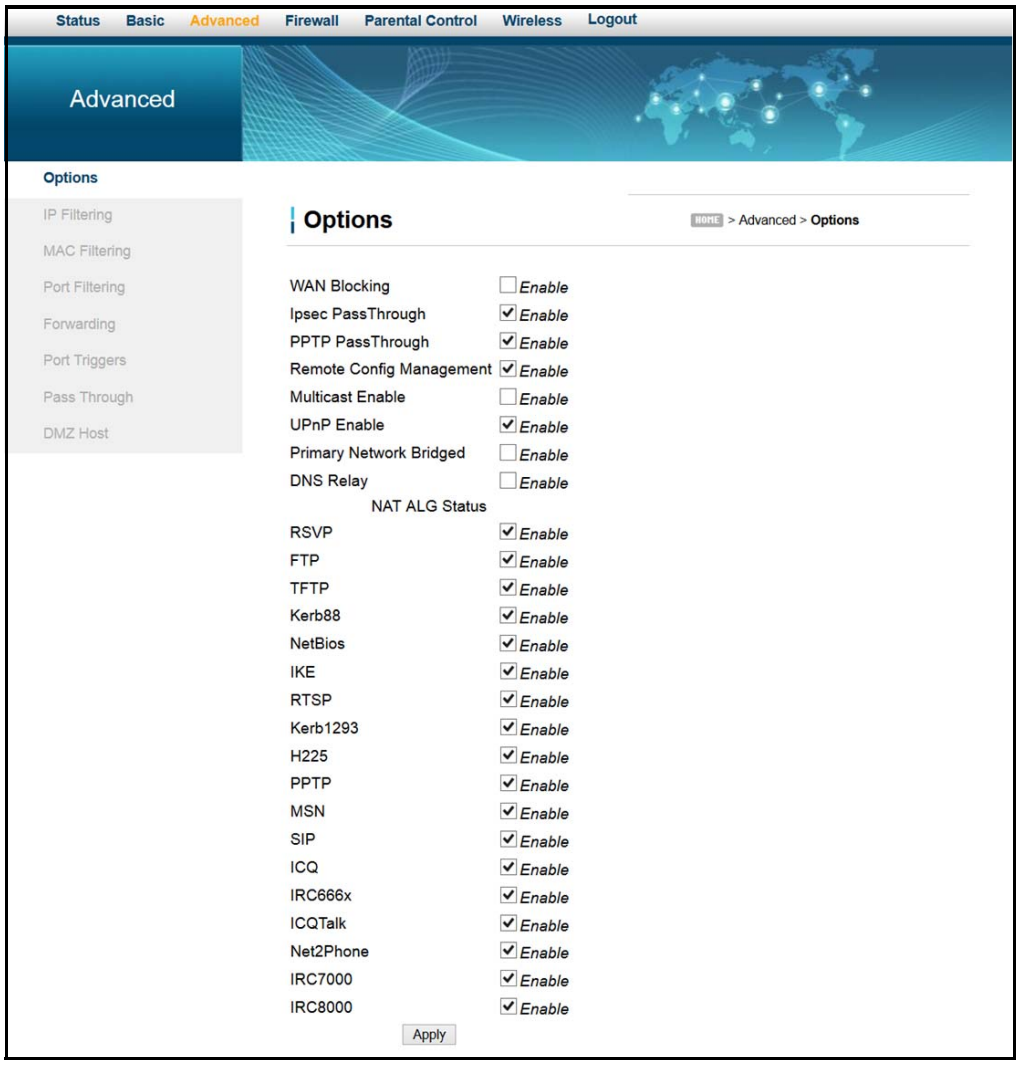
6.1 Using the Options Option

Use the **Options** option to define which networking protocols are enabled or disabled on the device. The network address translation application-level gateway (NAT ALG) settings provide additional security beyond the firewall.

Steps

To enable or disable network protocols:

1. Click **Advanced** from the main menu.
2. Click **Options** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
WAN Blocking	Blocks connection requests initialized from Internet users when enabled. WAN Blocking must be disabled to be able to PING the WAN gateway IP.
Ipsec PassThrough	Forces the router to redirect the IPSec request to the local host when enabled. NAT fails this attempt if Internet users initialize an IPSec VPN request to a host located behind the router.
PPTP PassThrough	Forces the router to redirect the PPTP request to the local host when enabled. NAT fails this attempt if Internet users initialize a PPTP VPN request to a host located behind the router.
Remote Config Management	Enables or disables access to the device from a remote system in order to configure settings. Remote management can be achieved by using SNMP, web/HTTP or telnet.
Multicast Enable	Optimizes the bandwidth utilization compared with unicast (especially video streaming applications).

Label	Description
UPnP Enable	Activates Universal Plug and Play (UPnP) when enabled. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. Gaming consoles and Web cameras are examples of devices that can use UPnP.
Primary Network Bridged	When enabled, all wireless traffic sourced from the primary SSID will be bridged.
DNS Relay	Allows the DDW365 to act as the “relay” device. Each PC that wants to access a URL does not have to send a DNS request to a DNS server on the Internet. DNS is used to resolve a URL (Web site name) to an IP address. DNS Relay is typically used for commercial applications where each device/PC connected to the device uses the DNS Relay address rather than going to a public DNS server hosted by an ISP to look up a URL.
NAT ALG Status – Filters to allow (enable) or disallow (disable) protocols to pass through the DDW365 to connected devices (computers, game consoles, and so on).	
RSVP	Enables or disables resource reservation protocol (RSVP). RSVP defines how applications reserve resources and how they free the reserved resources once they are no longer needed.
FTP	Enables or disables the file transfer protocol (FTP) used to transfer files from one host to another.
TFTP	Enables or disables the trivial file transfer protocol (TFTP) – a simpler protocol generally used for automated file transfers.
Kerb88	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 88 to prove their identity to one another.
NetBios	Enables or disables the network basic input/output system (NetBIOS) services related to the OSI session layer. NetBIOS allows applications on separate computers to communicate over a LAN.
IKE	Enables or disables the network key exchange (IKE) protocol used to set up a security association (SA) in the IPsec protocol suite.
RTSP	Enables or disables the real time streaming protocol (RTSP) network control protocol used to establish and control media sessions between end points.
Kerb1293	Enables or disables the Kerberos network authentication protocol which allows nodes to communicate over a non-secure network using “tickets” on port 1293.
H225	Enables or disables the H.225 protocol used to define messages and procedures for call signaling, media packetization, and registration, admission, and status (RAS) functions.

Label	Description
PPTP	Enables or disables the point-to-point tunneling protocol (PPTP) used to implement a virtual private network.
MSN	Enables or disables the Microsoft network protocol used for instant messaging.
SIP	Enables or disables the session initiation protocol application layer gateway (SIP ALG). SIP ALG inspects protocol packets and formats SIP message headers and SDP body to ensure proper signaling. **Note:** Some hosted VoIP services prefer this function to be performed by their own session border controller (SBC) and require the SIP ALG to be disabled. Some IP-PBXs may require SIP ALG enabled.
ICQ	Enables or disables the ICQ instant messaging program.
IRC666x	Enables or disables the Internet relay chat (IRC) protocol used for text messaging.
ICQTalk	Enables or disables the ICQTalk instant messaging program.
Net2Phone	Enables or disables Net2Phone SIP- and PacketCable-based VoIP.
IRC7000	Enables or disables the Internet relay chat protocol on TCP port TCP 7000 used for text messaging and group forums.
IRC8000	Enables or disables the Internet relay chat protocol on UDP port 8000 used for text messaging and group forums.
Apply	Saves changes.

6.2 Using the IP Filtering Option

Use the **IP Filtering** option to filter IP addresses to block Internet traffic to specific network devices on the LAN. Any host on this list is not accessible to Internet traffic.

Note

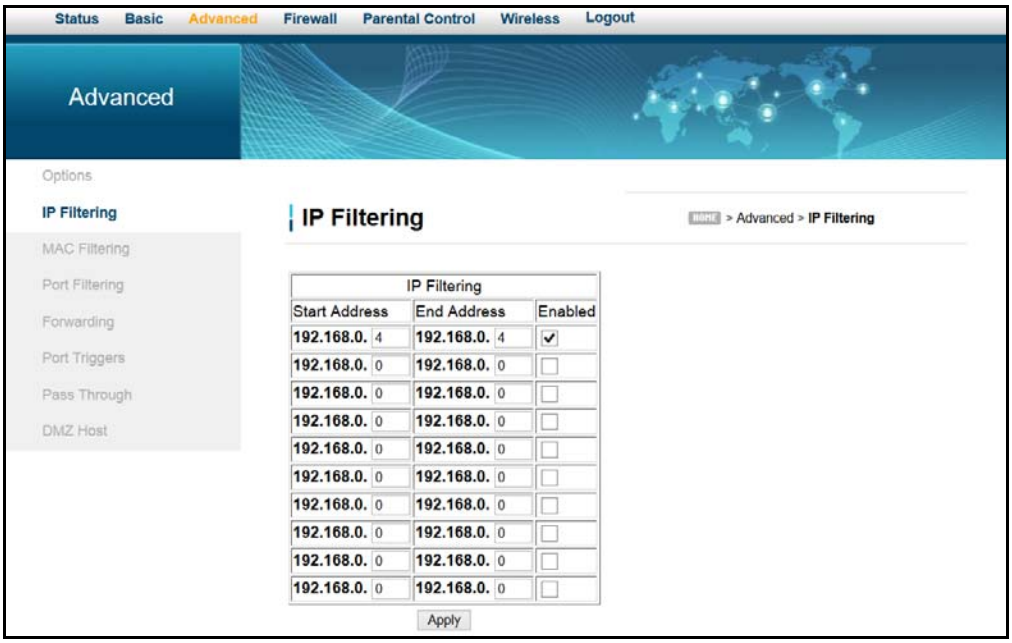
You may also filter by the MAC address which does not require setting a static lease. Refer to Using the MAC Filtering Option on page 40.

Steps

To filter IP addresses:

1. Make sure a PC is connected to the DDW365 and both devices are powered on and functioning.
2. Log in to the DDW365 Web user interface. Refer to Accessing the Web User Interface Locally on page 13.
3. Click **Advanced** from the main menu.

4. Click **IP Filtering** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Start Address	Defines the starting IP address to block.
End Address	Defines the ending IP address to block.
Enabled	Activates the rule when enabled is checked.
Apply	Saves changes.

6.3 Using the MAC Filtering Option

The **MAC Filtering** option allows you to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the DDW365.

Steps

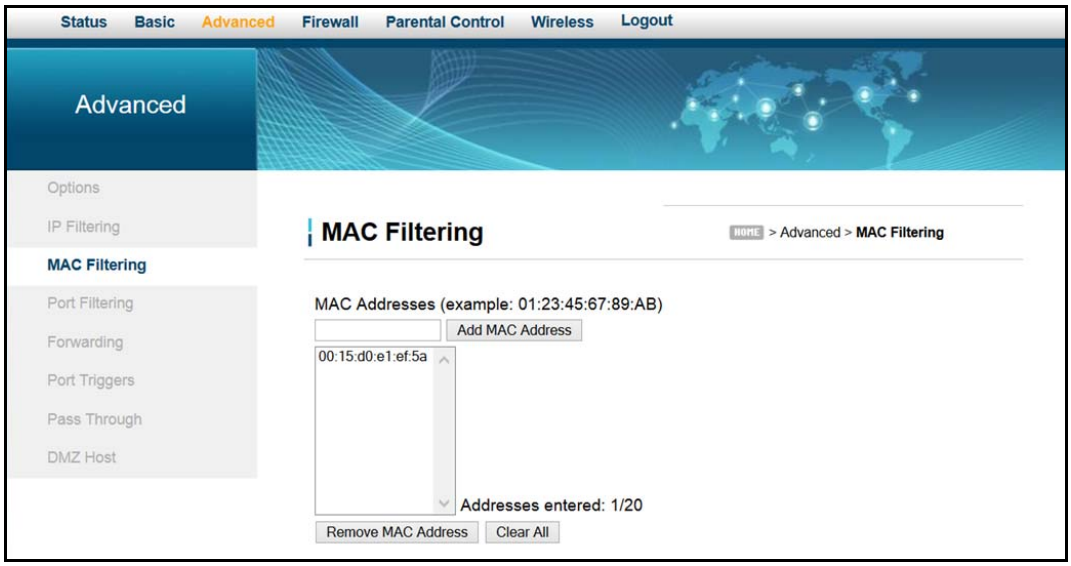
To filter MAC addresses:

1. Note the MAC addresses of the devices that you want to deny Internet access.

   Be sure all devices to which you potentially deny Internet access are connected to the DDW365 network.

2. Click **Advanced** from the main menu.
3. Click **MAC Filtering** from the left side menu.

4. Enter the MAC address to block in the text box to the left of the **Add MAC Address** button.
5. Click the **Add MAC Address** button. The MAC address is displayed in the filtered MAC address list. Field descriptions are listed below the screen example.



Label	Description
MAC Addresses	Defines the MAC address to block. Enter the MAC address in the field.
Add MAC Address	Adds the MAC address to the list of addresses to block.
Addresses entered: n/20	Displays the MAC addresses to be blocked. The number of MAC addresses entered is shown as 1/20 where 1 is the number of addresses in the list. You can filter up to twenty MAC addresses at one time.
Remove MAC Address	Deletes the selected MAC address from the list of addresses to be blocked.
Clear All	Removes all MAC addresses from the list.

6.4 Using the Port Filtering Option

Use the **Port Filtering** option to configure port filters to block to all devices on the LAN Internet services that use the ports specified.

Steps

To configure port filters:

1. Click **Advanced** from the main menu.
2. Click **Port Filtering** from the left side menu. Field descriptions are listed below the screen example.

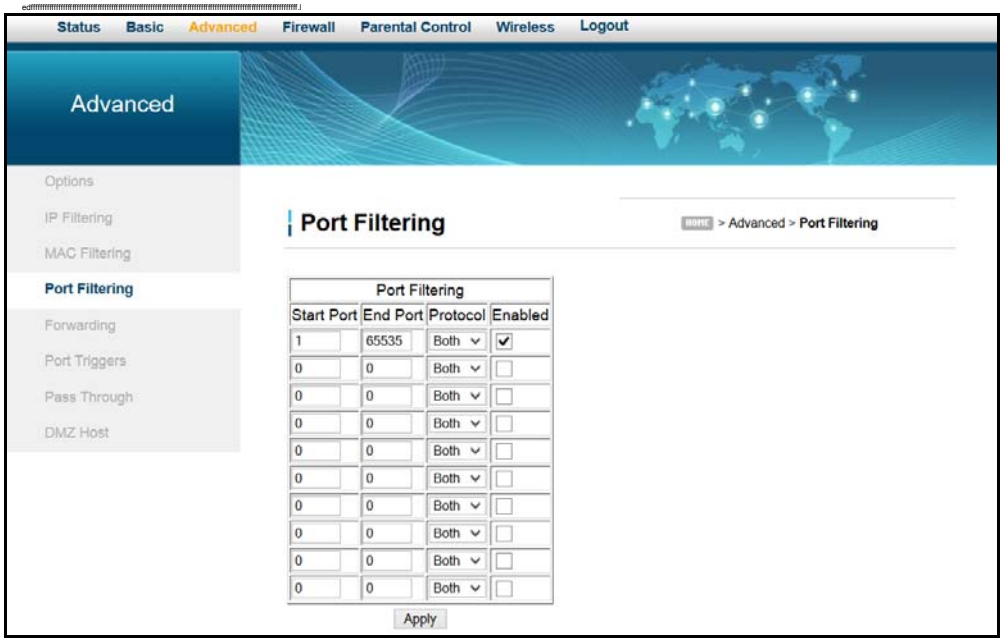
For example:

To prevent all Telnet access into and across your LAN:

1. Enter the **Start** and **End** ports to be 23.
2. Select **Both** for Protocol to include TCP and UDP.
3. Check **Enabled**.
4. Click **Apply**. Field descriptions are listed below the screen example.

Caution

Use caution when assigning port filtering by port range. You may accidentally prevent traffic that should pass through your network, such as http or email. Pre-assigned application ports are displayed on the Forwarding screen. Refer to Using the Forwarding Option on page 43.



Label	Description
Start Port	Defines the starting port number
End Port	Defines the ending port number.
Protocol	Selects the protocol type. Options are UDP, TCP, or Both.
Enabled	Activates the rule and filters out all traffic on the specified ports.
Apply	Saves changes.

6.5 Using the Forwarding Option

Forwarding tells the DDW365 to which computer on the local area network to send data. If your host systems or applications have communications issues with the Internet, you can use forwarding to resolve the following issues:

- ❑ Data is sent from a local host to the Internet, but the return path of expected data is not received by your local host.
- ❑ An application or service running on your local network (on local host) cannot be accessed from the Internet directly (for example, a request to a local audio server). Examples are:
  - ♦ Xbox/PlayStation – Games/applications
  - ♦ Home Security Systems – Security systems that use the Internet
  - ♦ Audio Servers/VoIP – Audio and VoIP applications and services

Topics

See the following topics:

- ♦ Before Setting Up Forwarding on page 43
- ♦ Setting Up Forwarding on page 44
- ♦ Setting Up Forwarding for an Xbox Example on page 46

6.5.1 Before Setting Up Forwarding

Try the following options before you assign forwarding rules:

1. Enable Universal Plug and Play (UPnP). This may resolve the issue you have without setting up forwarding rules.
   a. Access the Web interface of the DDW365, see Accessing the Web User Interface Locally on page 13.
   b. Click **Advanced** from the main menu.
   c. Click **Options** from the left menu.
   d. Check the **Enable UPnP** box

   e. Click **Apply**.
   f. Test your local host or application such as your Xbox to see if it is functioning properly. Continue with port forwarding if the host or application is not communicating correctly.

2. Assign a Static IP lease to the client/host to which you are setting up forwarding. This way, the IP does not change and disrupt your forwarding rules. For example, if you are hosting a Web server in your internal network, and you wish to setup a forwarding rule for it, assign a static IP lease to that system to keep the IP from renewing and disrupting the forwarding rule.

6.5.2 Setting Up Forwarding

If the suggestions in Before Setting Up Forwarding on page 43 did not correct your communication problem, use port forwarding.

You need the following information to set up port forwarding:

- **IP address** of each local host system (for example, Xbox) for which you need to setup a port forwarding rule.
- **Port numbers** the local host's application listens to for incoming requests/data (for example, a game or other service). These port numbers should be available in the documentation associated with the application.

Note

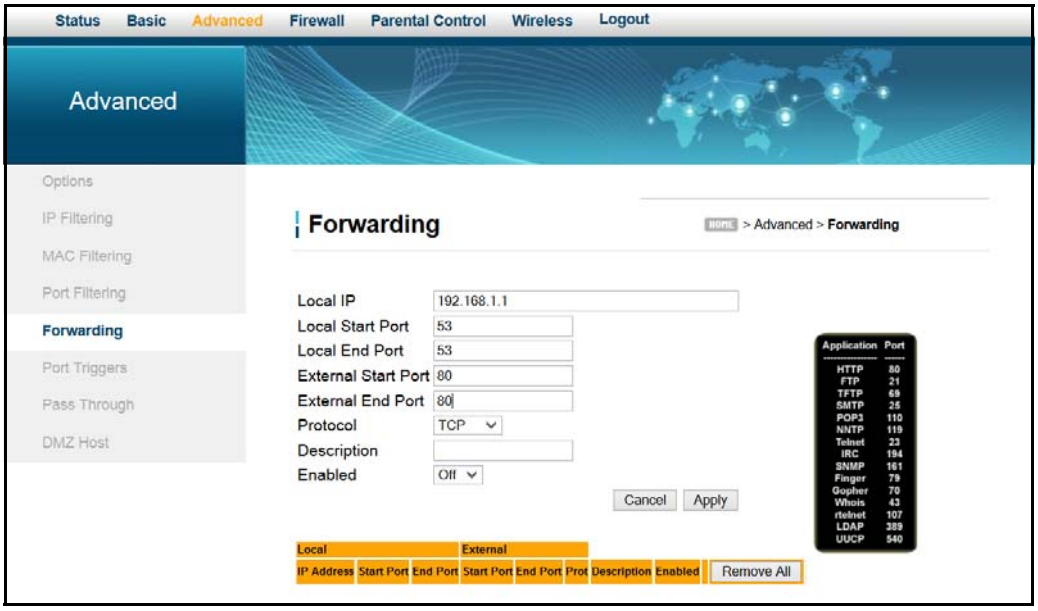
For detailed information on port forwarding, including how to set it up for specific applications using specific network devices (for example, cable modems), refer to: http://portforward.com or consult your host device or application user manual.

Steps

To set up forwarding:

1. Access the Web interface of the DDW365, see Accessing the Web User Interface Locally on page 13.
2. Click **Advanced** from the main menu.
3. Click **Forwarding** from the left menu.
4. Click **Create IPv4.**

5. Enter information in the forwarding fields as shown in the screen shot below. Field descriptions follow.

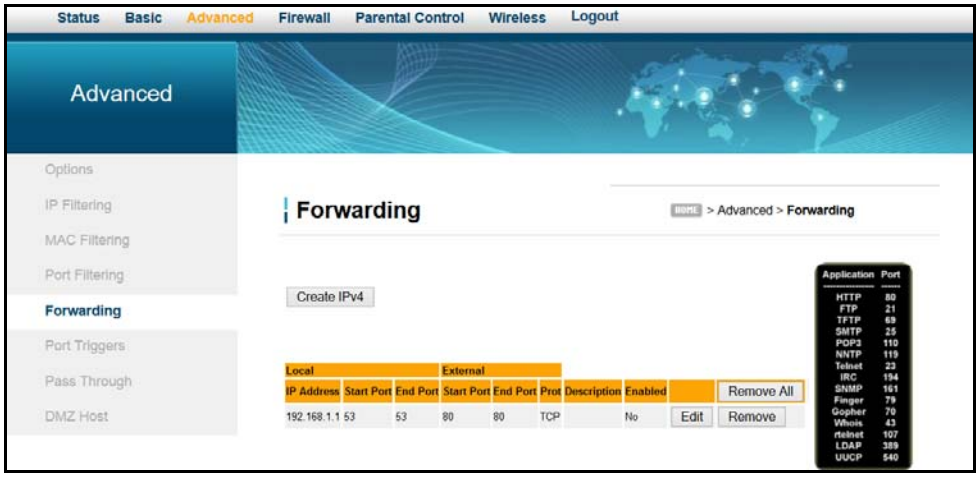


Label	Description
Local IP	Defines the IP address of the local LAN device to which the forwarding rule applies. For example, an Xbox or PC.
Local Start Port	Defines the starting port number listened to by the server host located in your LAN.
Local End Port	Defines the ending port number listened to by the server host located in your LAN.
External Start Port	Defines the port number to start the range of ports to publish to the Internet.
External End Port	Defines the port number to end the range of ports published to Internet. Note: Be very careful with ranges. Ports within a range are not usable by other applications that may require them. It is common and safer to enter the same port number as the start and end of the range.
Protocol	Selects the protocol type. Options are UDP, TCP, or BOTH.
Description	Names the forwarding rule.
Enabled	Disables (Off) or enables (On) the forwarding rule.
Cancel	Stops creating the forwarding rule and returns you to the previous Forwarding screen.
Apply	Saves changes.
Port Map	Shows a list of common applications and their ports.

Forwarding Table – Lists existing forwarding rules.

Remove All	Deletes all entries in the forwarding table.
Remove	Deletes the rule selected.

6. Click **Apply**. The forwarding rule is created and displayed in the table as shown below. Additional field descriptions follow.



Label	Description
Edit	If Edit is selected, fields for the rule selected will be displayed. Values can then be changed.
Remove	Deletes the selected rule.

6.5.3 Setting Up Forwarding for an Xbox Example

Following is an example of how you would set up a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set for each port. Multiple ports and forwarding rules may not be required for other applications.

Steps

To set up port forwarding for an Xbox:

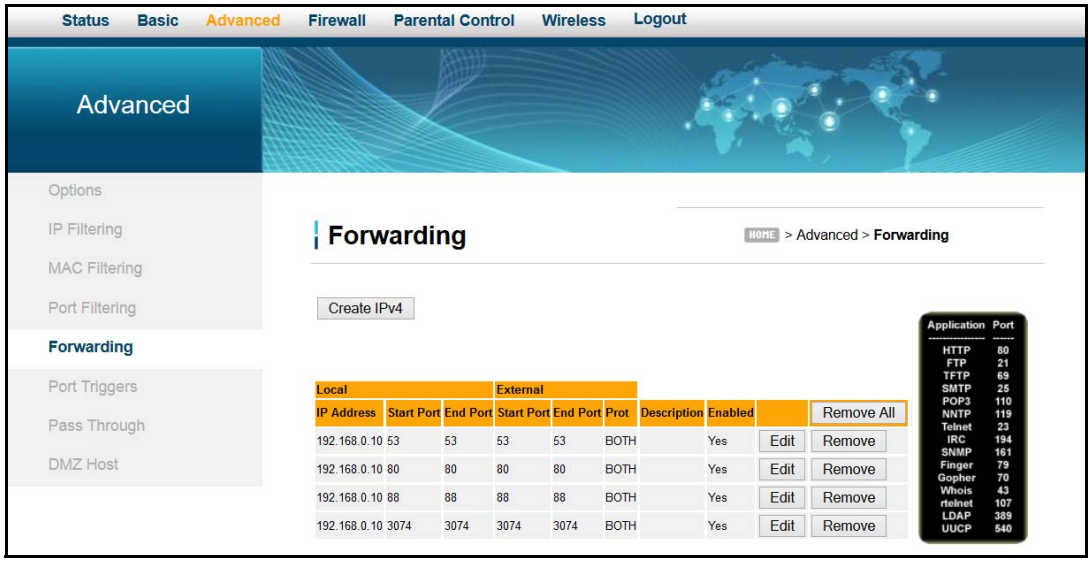
1. Click **Advanced** from the main menu.
2. Click **Forwarding** from the left side menu.
3. Enter the Xbox IP address in the **Local IP** field.
4. Define ports used by the Xbox in the **Local Start Port** and **Local End Port** fields. Define the same ports used by the Xbox in the **External Start Port** and **External End Port** fields.

5. Create Port Forwarding rules per port. A rule set up for port 53 works only for port 53. A port can be used only by one program at a time.

Note

You can set up applications/services to listen on one internal port. External Internet users who want to access that application, address it using an external port, such as an Audio server. Internal Ports are the ports to which local servers listen. External Ports are the ports that the cable modem listens to from the WAN.

The following screen shot shows Forwarding set up for an Xbox.



6.6 Using the Port Triggers Option

Port Triggers define dynamic triggers to specific devices on the LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

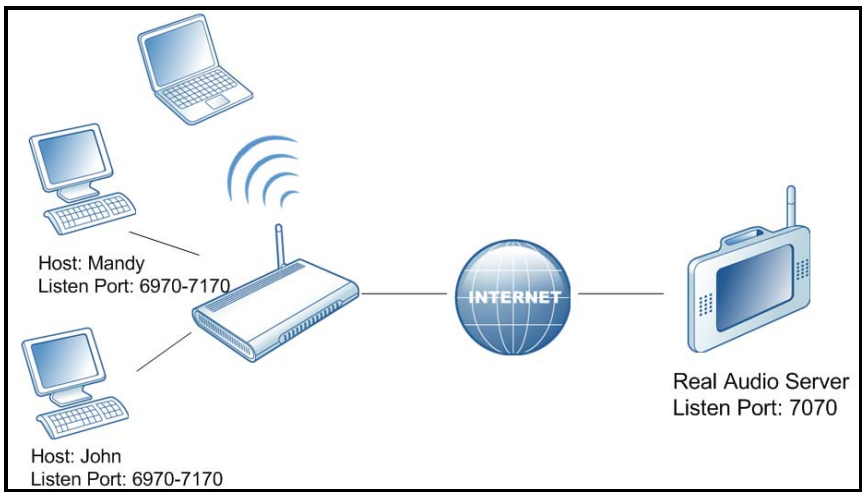
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. The difference between port forwarding and triggering is:

- Port forwarding sets a rule to send a service to a single LAN IP address.
- Port triggering defines two kinds of ports: trigger port and target port. The trigger port sends a service request from a LAN host to a specific destination port number. The port the LAN host is required to listen to by the application is called the target port. The server returns responses to these ports.

For example:

1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The DDW365 associates John's computer IP address with the “target” port range of 6970-7170.

2. The Real Audio server responds to a port number ranging between 6970-7170.
3. The DDW365 forwards the traffic to John's computer IP address.
4. Only John can connect to the Real Audio server until the connection is closed or expires.



Steps

To set up port triggering:

1. Click **Advanced** from the main menu.
2. Click **Port Triggers** from the left side menu.
3. Click **Create** and enter information in the trigger fields.
4. Click **Apply**. The port trigger rule is created and displayed in the table. Field descriptions are listed below the screen example.

Note

The following example shows the Port Triggering option set up for a dual Xbox configuration.

Label	Description
Trigger Start Port	Defines a port number or the starting port number in a range of port numbers.
Trigger End Port	Defines a port number or the ending port number in a range of port numbers.
Target Start Port	Defines a port number or the starting port number in a range of port numbers.
Target End Port	Defines a port number or the ending port number in a range of port numbers.
Protocol	Defines the protocol type for this rule, UDP, TCP, or Both.
Description	Names the triggering rule.
Enabled	Enables (on) or disables (off) the triggering rule.
Apply	Saves changes.

6.7 Using the Pass Through Option

Use the **Pass Through** option to configure a pass through table. Devices in the pass through table are treated as bridge devices, storing and forwarding data between LAN interconnections.

Steps

To configure a pass through table:

1. Click **Advanced** from the main menu.
2. Click **Pass Through** from the left side menu. The pass through fields are explained following this screen example.

Label	Description
Pass Through MAC Addresses	Defines the input host's MAC address.
Add MAC Address	Adds the input host's MAC address.
Addresses entered: n/32	Displays the MAC addresses to be blocked. The number of MAC addresses is shown as 0/32 where 0 is the number of addresses in the list. You can add up to 32 MAC addresses at one time.
Remove MAC Address	Removes the input host's MAC address.
Clear All	Removes all of the input host's MAC addresses.

6.8 Using the DMZ Host Option

Use the **DMZ** (Demilitarized Zone) **Host** option to expose a host IP address to the WAN (public Internet). You can use this option when applications do not work with port triggers or other networking strategies.

Steps

To set up a DMZ host:

1. Connect a PC to an Ethernet port on the DDW365. Make sure both devices are powered on and functioning.
2. Connect a Home Gateway (or other device you wish to be in the DMZ) to an Ethernet port on the DDW365.
3. Log in to the DDW365 Web user interface.
4. Click **Advanced** from the main menu.
5. Click **DMZ Host** from the left side menu.
6. Enter the IP address of the Home Gateway (host device) to be exposed to the WAN.
7. Test the device to ensure Internet access is available and the device is functional. For

example, connect to the Internet from a PC connected to the Home Gateway.

Label	Description
DMZ Address	Defines the IP address of the host to be exposed.
Apply	Saves changes.

7 Understanding the Firewall Menu

Use these instructions to configure the DDW365 firewall settings to control what types of traffic are allowed on your network. The firewall can block certain Web-oriented cookies, Java scripts, and pop-up windows. It is highly recommended the Firewall is left enabled at all times to protect against denial of service (DoS) attacks. Refer to Using the Basic Option on page 52 to block Internet access to specific sites.

Note: Firewall menu options are not available when the device is in Bridge mode.

Topics

See the following topics:

- Using the Basic Option on page 52
- Using the Local Log Option on page 53
- Using the Remote Log Option on page 54

Steps

To access the firewall menu:

1. Access the Web user interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click **Firewall** from the main menu.

7.1 Using the Basic Option

Use the **Basic** option to filter Web content to block certain Web-oriented cookies, Java scripts, and pop-up windows.

Steps

To filter Web content:

1. Click **Firewall** from the main menu.
2. Click **Basic** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
IPv4 Firewall Protection	Defines the level of protection. Choices are Off, Low, Medium, and High. Services are based on the protection level and displayed in the Allowed Services window.
Block Fragmented IP Packets	Detects fragmented IP packets and blocks them.
Port Scan Detection	Detects port scans that probe for available ports and potentially use these ports to detect weakness in the network.
IP Flood Detection	Detects IP flood attacks that send excessive information to the device, using up bandwidth.
Apply	Saves changes.

7.2 Using the Local Log Option

Use the **Local Log** to define firewall event log reporting through email alerts and report on possible attacks on the system.

Steps

To define local log reporting:

1. Click **Firewall** from the main menu.
2. Click **Local Log** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
Contact Email Address	Defines the email address where you want to send the log.
SMTP Server Name	Defines the name of the SMTP server, such as smtp.example.com.
SMTP Username	Defines the username for the email address, such as smtp.username.
SMTP Password	Defines the password for the email address.
E-mail Alerts	Enables or disables log reporting.
Apply	Saves the settings and completes the setup.
E-mail Log	Sends the log to the specified email address.
Clear Log	Deletes the log.

7.3 Using the Remote Log Option

Use the **Remote Log** option to define events and send the log to a local SysLog server.

Steps

To configure the firewall remote log:

1. Click **Firewall** the main menu.
2. Click **Remote Log** from the left side menu. The **Remote Log** fields are explained following this screen example.

Label	Description
Permitted Connections	Logs all access attempts that are allowed by the firewall.
Blocked Connections	Logs all access attempts that are blocked by the firewall.
Known Internet Attacks	Logs all known attacks from the Internet.
Product Configuration Events	Logs when the DDW365 is configured/modified by a user or administrator.
to SysLog server at 192.168.0.	Defines the IP address of the Syslog server.
Apply	Saves changes.

8 Understanding the Parental Control Menu

Parental Controls allow you to control Internet access for users on the DDW365 network. Parental Controls provides the following features:

- Define user/password access.
- Block specific Web sites and Web sites based on keywords.
- Define the times users are allowed to access the Internet.
- View a local log to view Internet activity.

Topics

See the following topics:

- Using the Parental Control User Setup Option on page 56
- Using the Basic Option on page 58
- Using the ToD Filter Option on page 60
- Using the Local Log Option on page 61

Steps

To access the parental control menu:

1. Access the Web interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click the **Parental Control** link from the top of the screen.

8.1 Using the Parental Control User Setup Option

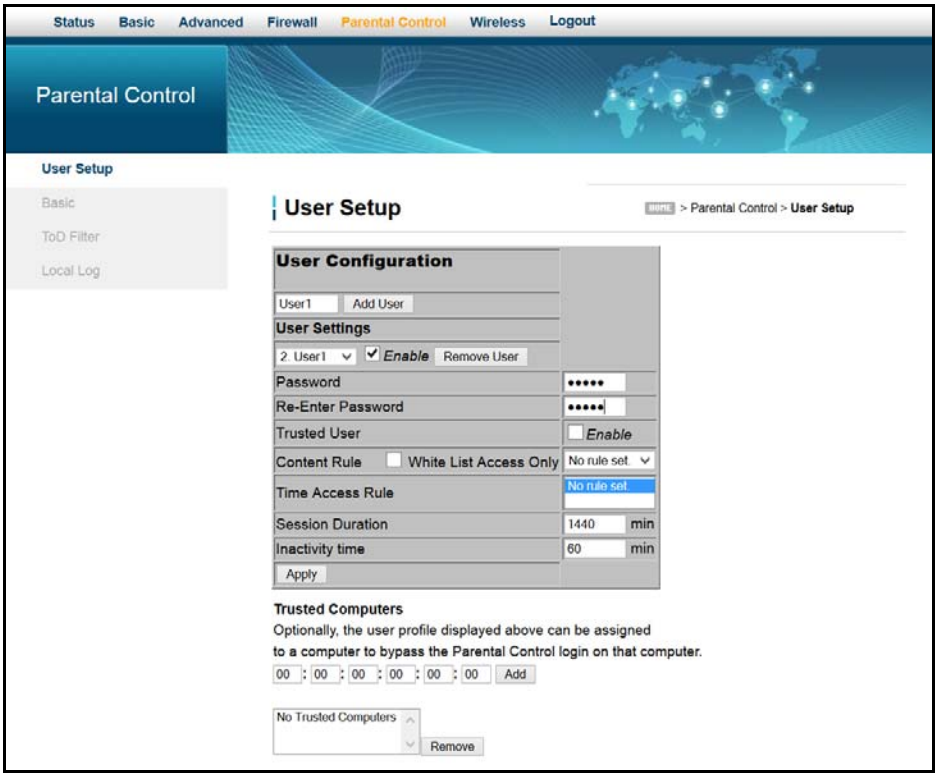
The **User Setup** option allows you to configure which user accounts can or cannot connect to your wireless or wired network, and the parameters of each connection.

Steps

To configure user accounts:

1. Click the **Parental Control** link from the top of the screen.
2. Click **User Setup** from the left side of the screen. The **User Setup** fields are explained following the screen example.

   Note: To enable Parental Control, refer to Using the Basic Option on page 58.



Label	Description
Add User **Remove User** **Enable**	Defines user accounts. ♦ To add a new user, type in the user name and click Add User. The user then becomes selectable in the User Settings drop-down menu. ♦ To select an existing user, choose the user from the User Settings drop-down menu. ♦ To activate the user, check Enable. ♦ To remove a user, select the user from the drop-down menu and click Remove User.
Password	Defines the password for this user. It is required when this user tries to access the Internet via the device.
Re-Enter Password	Confirms the password with the re-entered password.
Trusted User	Defines the selected user as a trusted user when enabled is checked. The user is limited to timing and content when visiting the Internet, as defined in the following fields.
Content Rule	Selects from the pop-up menu an existing content rule that defines what kind of Websites the user can visit or not.
White List Access Only	Selects the White List Access option. If you have created a content rule that defines a black list and white list, select the White List Access Only checkbox to force the DDW365 to execute the policy for the selected user.
Time Access Rule	Selects a defined time access rule to apply to the selected user.

Label	Description
Session Duration	Allows you to enter a time in minutes for the user's session to expire. When the session expires, the user can log in again for the same session duration.
Inactivity Time	Allows you to enter the time out value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is canceled.
Apply	Saves all changes when clicked.
Trusted Computers	Defines the trusted hosts that can bypass the Parental Control Process.
Add	Adds the trusted host's MAC address entered in the given area and Add is clicked.
Remove	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

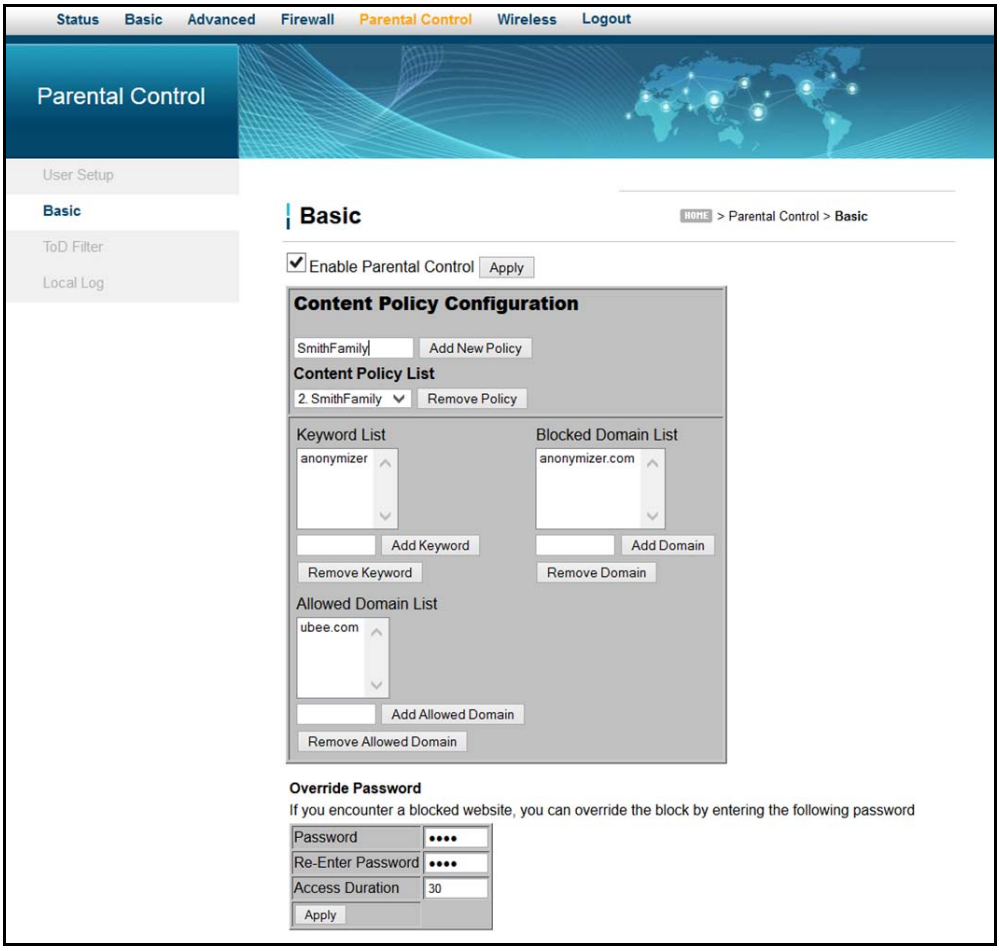
8.2 Using the Basic Option

The **Basic** option allows you to select rules to block certain Internet content and Web sites. After you change your Parental Control settings, click the appropriate Apply, Add, or Remove button for your new settings to take effect. Refresh your browser's display to see the currently active settings.

Steps

To filter Internet content and Web sites:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Basic** from the left side of the screen. The **Basic** fields are explained following this screen example.



Label	Description
Enable Parental Control	Activates the Parental Control feature when checked.
Apply	Saves all changes in the screen and activates Parental Control, if enabled.
Content Policy Configuration	
Add New Policy	Adds a policy to the Policy List. Enter the policy name and click Add New Policy.
Content Policy List	Lists existing policies you can choose to use.
Remove Policy	Deletes a policy from the list. Select the policy from the list and click Remove Policy.
Keyword List	Displays keywords you can use to block Web site addresses (URLs) containing those words.
Add Keyword	Adds a keyword to the keyword list. Enter the word in the field next to the Add Keyword button and click Add Keyword. The keyword is added to the list.
Remove Keyword	Removes a keyword from the keyword list. Select the keyword from the list, and click Remove Keyword.

Label	Description
Blocked Domain List	Displays Web domains (for example, unwanted.com) you can use to block access to those domains.
Add Domain	Adds a domain to the Allowed Domain List. Enter a domain, and click Add Domain.
Remove Allowed Domain	Removes a domain from the Allowed Domain List. Select the domain from the list, and click Remove Domain.
Allowed Domain List	Displays domains you have added as Allowed Domains.
Add Allowed Domain	Adds allowed domains to the list. Enter the name and click Add Allowed Domain.
Remove Allowed Domain	Removes domain names from the list. Highlight the domain from the list and click Remove Allowed Domain.
Override Password	If you encounter a blocked website, you can override the block by entering a password.
Password	Enter a password for overriding blocked websites.
Re-Enter Password	Re-enter the password.
Access Duration	Set a time duration (in minutes) for access to the blocked site when the block has been overridden by entering the password.
Apply	Saves the password and access duration time.

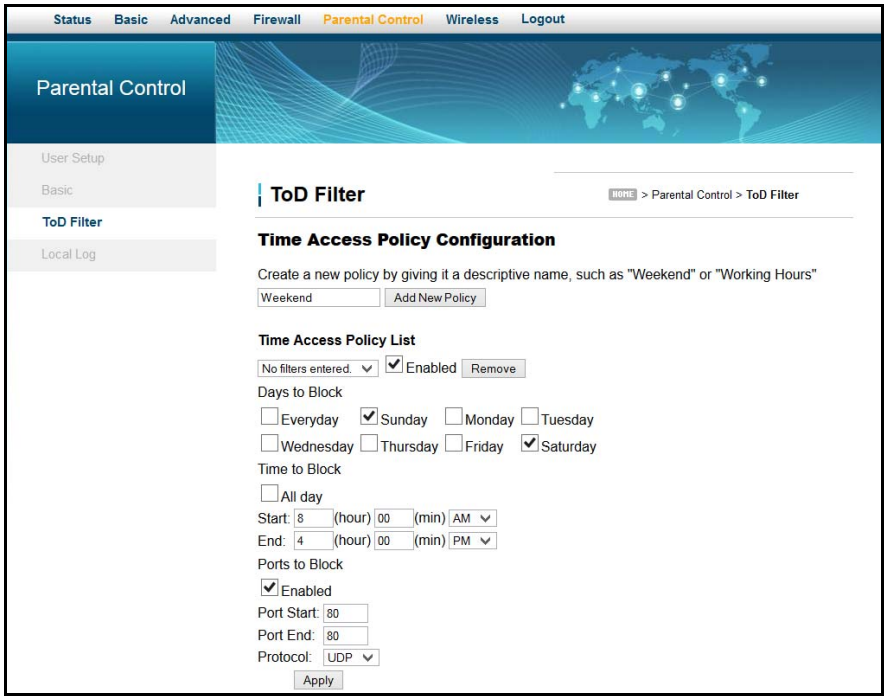
8.3 Using the ToD Filter Option

The **ToD** (Time of Day) **Filter** option allows the configuration of time-based access policies to block all Internet traffic at specified times.

Steps

To configure ToD filters:

1. Click the **Parental Control** link from the top of the screen.
2. Click **ToD Filter** from the left side of the screen. The **ToD Filter** fields are explained following this screen example.



Label	Description
Add New Policy	Adds a new policy. Enter a policy name and click the Add New Policy button.
Time Access Policy List	Lists the existing policies in a drop-down list.
Enabled	Activates a policy. Select the policy from the drop-down list and check Enabled.
Remove	Deletes a policy. Select the policy from the drop-down list and click Remove.
Days to Block	Selects the days to block Internet access.
Time to Block: **All Day or a specific time frame**	Defines the time to block. ♦ To block all day, check All Day to eliminate all access during the days selected. ♦ To block a specific time frame for the days selected, enter the Start time and the End time. Select AM or PM for each.
Ports to Block	Defines a port range to block if the Enabled box is checked. ♦ Port Start: Enter the starting port number to be blocked. ♦ Port End: Enter ending port number to be blocked. ♦ Protocol: Select the protocol type. Options are UDP, TCP, or Both.
Apply	Saves all changes when clicked.

8.4 Using the Local Log Option

The **Local Log** option displays Parental Control event log reporting.

Steps

To view the parental control local log:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Local Log** from the left side of the screen. The **Local Log** fields are explained following this screen example.

Label	Description
Last Occurrence	Displays the time when the last event occurred.
Action	Displays what is done by parental control, including dropping or permitting access requests.
Target	Displays the destination IP address of a certain access request.
User	Displays the user who triggered this event log.
Source	Displays the source IP address of this event.
Clear Log	To empty the displayed log entries, click Clear Log.

9 Understanding the Wireless Menu

Use the Wireless menu to configure a wireless network.

Topics

See the following topics:

- Using the Wireless Radio Option on page 63
- Using the Primary Network Option on page 66
- Using the Access Control Option on page 70
- Using the Wi-Fi Multimedia Option on page 72
- Using the Bridging Option on page 75
- Deploying and Troubleshooting the Wireless Network on page 76

Steps

To access the wireless menu:

1. Access the Web interface. Refer to Accessing the Web User Interface Locally on page 13.
2. Click **Wireless** from the main menu.

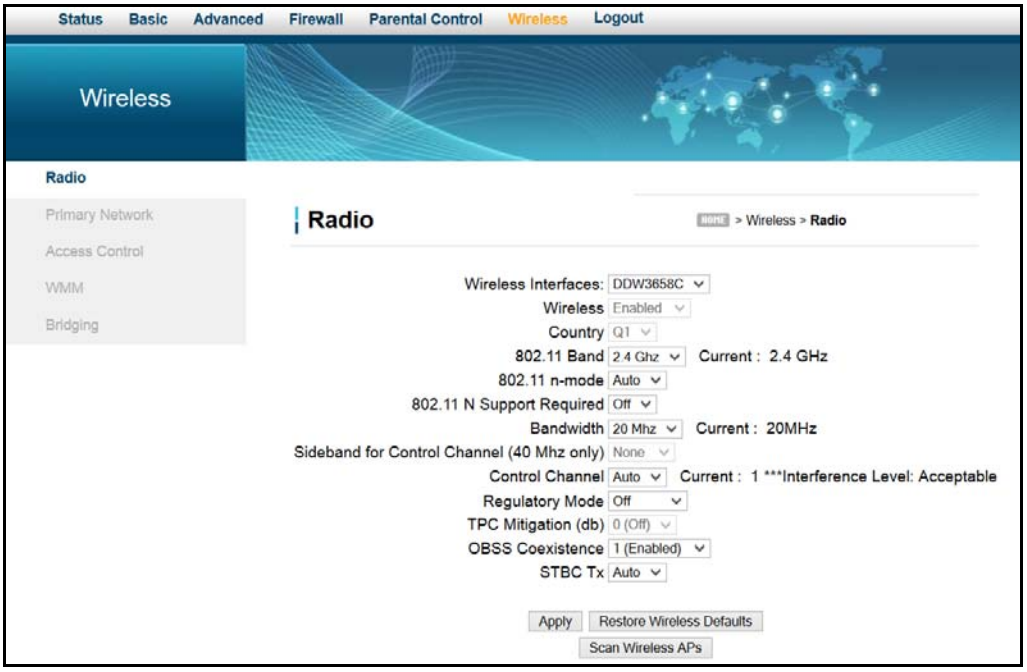
9.1 Using the Wireless Radio Option

The **Radio** option is used to configure the wireless radio, including channel number, and bandwidth control.

Steps

To configure wireless operations:

1. Click **Wireless** from the main menu.
2. Click **Radio** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Wireless Interfaces	Displays the primary SSID. The default SSID is “DDW365” plus the last 2 characters of the MAC address with the letters entered in UPPER case.
Wireless	Displays the wireless radio’s status, Enabled or Disabled.
Country	Defines the country where this device is used. The default is Q1.
802.11 Band	Displays the 802.11 band (2.4GHz).
802.11 n-mode	Sets the wireless networking standard. By default it is set to Auto for 802.11 n mode. This mode has a significant increase in the maximum raw OSI physical layer data rate from 54 Mbit/s to a maximum of 600 Mbit/s with the use of four spatial streams when at a channel width of 40MHz. One spacial stream at 20MHz wide channel enables 72.2Mbps maximum data rate in 802.11n mode.
802.11 N Support Required	Defines whether 802.11n support is required (on) or not (off). On forces the device to 802.11n mode and clients must support 802.11n.
Bandwidth	Sets the bandwidth to 20Mhz or 40Mhz. For 40MHz, set the sideband to lower or upper 20Mhz. 40 MHz channels double the channel width. This allows doubling the PHY data rate over a single 20 MHz channel. The default is 20MHz.
Sideband for Control Channel (40MHz only)	Only when using 40MHz Bandwidth should you choose the Lower or Upper 20MHz.

Label	Description
Control Channel	Set to Auto by default, the Control Channel selects a specific channel to deploy the wireless network. This allows you to set the operating frequency/channel depending on your particular region. Channel selection can have an impact on wireless networking performance. For more information, refer to Selecting a Wireless Channel on page 79
Regulatory Mode	Defines whether Regulatory Mode is set to off, 802.11d, or 802.11h.
TPC Mitigation (dB)	Defines the transmitter power control (TPC) mitigation setting as 0 (off), 2,3, or 4.
OBSS Coexistence	Enables or disables overlapping BSS coexistence.
STBC Tx	Sets the space-time block codes (STBCs) for the transmitting antenna.
Apply	Saves all screen changes when clicked.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations when clicked.
Scan Wireless APs	Scans for other wireless access points and displays channel, encryption, SSID, RSSI levels, and other information. See the section below for more information.

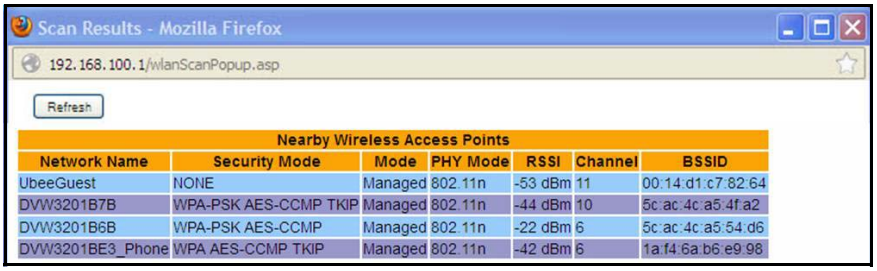
9.1.1 Scanning for Wireless Access Points (APs)

You can search for wireless access points and display the results in a new window.

Steps

To search for wireless access points:

1. Click **Scan Wireless APs** at the bottom of the Wireless Radio screen. Results are displayed in a new window.


Scan Results - Mozilla Firefox
192.168.100.1/wlanScanPopup.asp
Refresh
Nearby Wireless Access Points
Network Name | Security Mode | Mode | PHY Mode | RSSI | Channel | BSSID
UbeeGuest | NONE | Managed | 802.11n | -53 dBm | 11 | 00:14:d1:c7:82:64
DVW3201B7B | WPA-PSK AES-CCMP TKIP | Managed | 802.11n | -44 dBm | 10 | 5c:ac:4c:a5:4f:a2
DVW3201B6B | WPA-PSK AES-CCMP | Managed | 802.11n | -22 dBm | 6 | 5c:ac:4c:a5:54:d6
DVW3201BE3_Phone | WPA AES-CCMP TKIP | Managed | 802.11n | -42 dBm | 6 | 1a:f4:6a:b6:e9:98

2. Click **Refresh** to update the results.

Label	Description
Network Name	Displays the name of the wireless network (SSID) broadcast by the access point.
Security Mode	Displays the encryption method used.
Mode	Displays the mode of the wireless access point: Possible modes are: ♦ Master – Communicates with associated wireless cards that are in managed mode. Appears as a normal access point with an SSID and channel. Network communications, such as authentication, conflict, and duplicate packets are managed by the wireless card. ♦ Managed – Communicates with an associated master, not directly with another managed AP. Wireless cards connect to the master network and change their channel to match. The master must accept the credentials of the managed network for it to be associated. ♦ Ad-hoc – Communicates directly with another wireless network. Network cards must be in range and use the same name and channel. ♦ Monitor – Communicates in observation mode and does not transmit. Can be used for troubleshooting wireless links or checking bandwidth usage in the area.
PHY Mode	Displays the physical transceivers (PHY) layer method used.
RSSI	Displays the received signal strength (RSSI) of the wireless access points in range of the device. Lower negative numbers (for example, -1 to -65) indicate the access point is closer. Greater negative numbers (for example, -66 to -95) indicate the access point is farther away.
Channel	Displays the channel on which the DDW365 is operating.
BSSID	Displays the MAC address for the nearby wireless access points.

9.2 Using the Primary Network Option

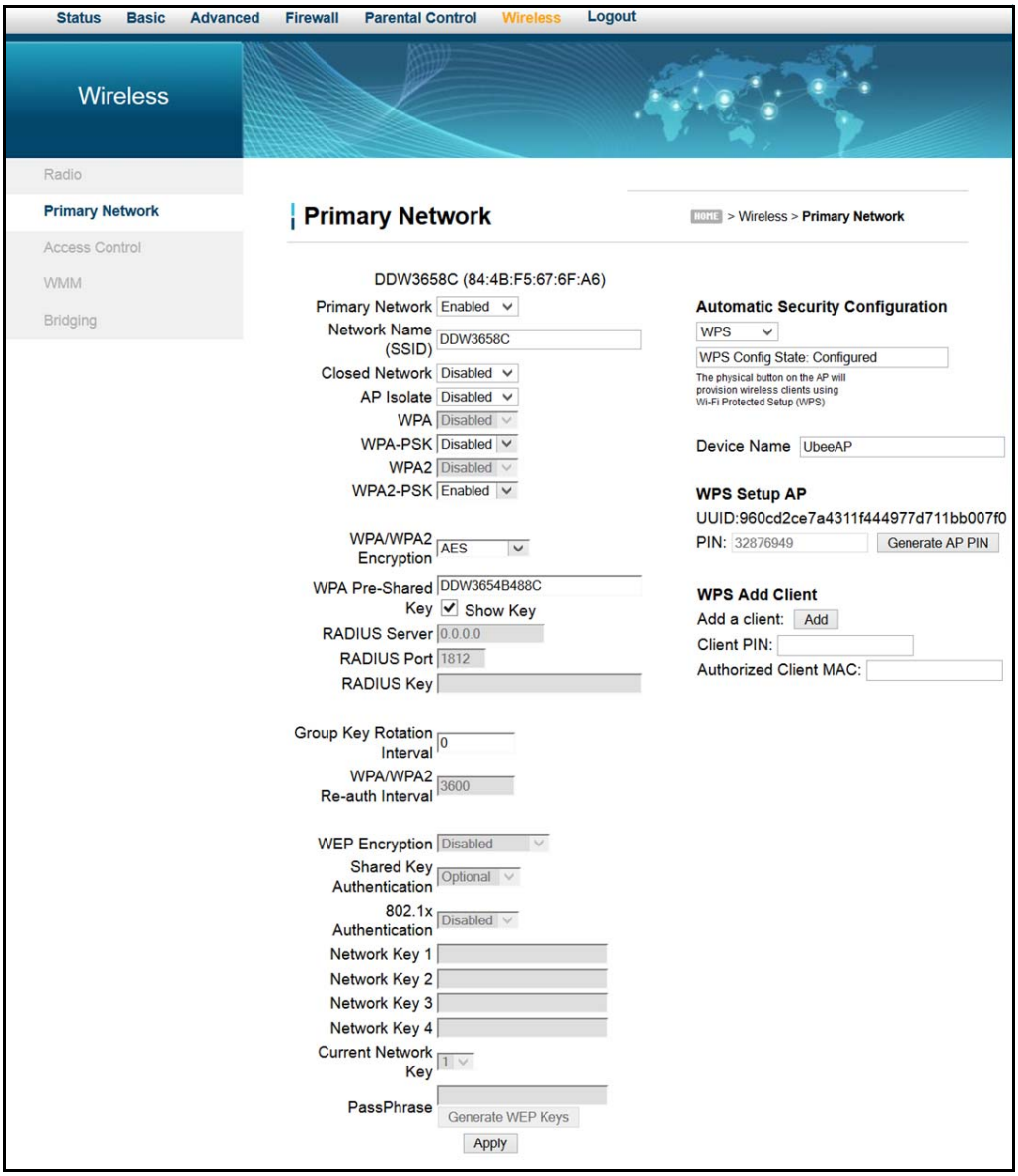
Use the **Primary Network** option to configure a variety of wireless security settings.

Steps

To configure wireless security options:

1. Click **Wireless** from the main menu.
2. Click **Primary Network** from the left side menu. Field descriptions are listed below the screen example. This example shows the settings when the modem is in the 2.4GHz band.

   Wireless default values are discussed in Understanding Default Values and Logins on page 8.



Label	Description
Primary Network	Enables or disables the primary network.
Network Name (SSID)	Defines the primary network name (SSID) to which client devices connect. The default SSID is “DDW365” plus the last 2 characters of the MAC address with the letters entered in UPPER case.
Closed Network	Hides the selected SSID when enabled so it is not visible to wireless clients unless manually set up on the client. If disabled, the SSID is visible. Closed Network is disabled by default to allow broadcasting of the primary network name (SSID). Refer to Enabling a Closed Network on the Primary Network on page 70 to set up a closed network. **Note:** WPS must be disabled before Closed Network can be enabled.

Label	Description
AP Isolate	Disabled by default. When enabled, it prevents wireless client stations from communicating with each other.
WPA	Enables or disables the Wi-Fi Protected Access (WPA) security protocol. WPA is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption. Setting WPA alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA-PSK	Enables or disables WPA Pre-Shared Key (WPA-PSK). If you do not have an external RADIUS server, use WPA-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN.
WPA2	Enables or disables WPA2. This advanced protocol is certified through Wi-Fi Alliance's WPA2 program and implements the mandatory elements of 802.11i. In particular, it has an AES-based algorithm (CCMP) that is considered fully secure. Setting WPA2 alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA2-PSK	Enables or disables WPA2-PSK. If you do not have an external RADIUS server, use WPA2-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the default residential subscriber setting. It is more secure than WPA-PSK and uses AES encryption.
WPA/WPA2 Encryption	Sets WPA/WPA2 encryption to AES or TKIP+AES. The default is AES.
WPA Pre-Shared Key	Displays the WPA key when “Show Key” is checked. The encryption mechanisms for WPA and WPA-PSK are the same, except that WPA-PSK uses a simple common password instead of user-specific credentials.
Show Key	Displays the pre-shared key when checked.
RADIUS Server	Defines the IP address of the RADIUS server, if used.
RADIUS Port	Defines a RADIUS port number when WPA or 802.1x network authentication is selected.
RADIUS Key	Defines the RADIUS Key when WPA or 802.1x network authentication is selected.
Group Key Rotation Interval	Allows the device to generate the best possible random group key and update all the key-management capable stations periodically. This field is set to 0 by default.

Label	Description
WPA/WPA2 Re-auth Interval	Sends a new group key to all clients at the specified interval for a wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management). The re-keying process is the WPA equivalent of automatically changing the WEP key for a wireless access point and all stations in the WLAN on a periodic basis. Setting the WPA Group Key Update Timer is also supported in WPA-PSK mode.
WEP Encryption	Enables or disables WEP encryption. If you do not have wireless clients that can use WPA or WPA2, you can use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the DDW365 to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the DDW365 must use the same WEP key. Data Encryption can be set to WEP **128-bit, 64-bit,** or **Disable.**
Shared Key Authentication	Defines Shared Key Authentication as optional or required. Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.
802.1x Authentication	Enables or disables 802.1x to authenticate wireless clients.
Network Key 1-4	Pre-defines up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits).
Current Network Key	Selects one of the four pre-defined keys as the current network key.
Passphrase	Sets the WEP encryption key by entering a word or group of printable characters in the Passphrase box and clicking Generate WEP keys. These characters are case sensitive.
Generate WEP Keys	Forces the device to generate 4 WEP keys automatically.
Apply	Saves changes.
Automatic Security Configuration — Sets up WPS (Wi-Fi Protected Setup) for devices connecting to the wireless network.	
WPS/Disabled	Enables or disables WPS option. When enabled, the following fields are available:
WPS Config State	Defines if the WPS has been configured or not.
Device Name	Defines a name for the DDW365 for WPS.
WPS Setup AP	
UUID	Defines the universal unique identifier (UUID) for this device.
PIN	Defines the Personal Identification Number for this device.
Generate AP PIN	Creates a new PIN for this device.

Label	Description
WPS Add Client	
Add a client	Activates wireless protected setup (WPS) security on the device. To add a client: 1. Click Add a client. The WPS Add Client screen is displayed. 2. Click PUSH on the WPS Add Client screen.The WPS button is activated on the device, indicated by a flashing white light on top of the unit. 3. Press the WPS button on the device.
Client PIN	Defines a PIN number for client access.
Authorized Client MAC	Defines the MAC address of the authorized client.

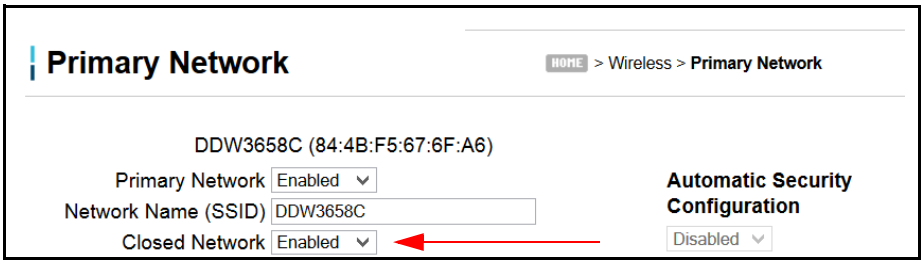
9.2.1 Enabling a Closed Network on the Primary Network

You can enable the Closed Network option so the SSID cannot be broadcast or seen by others.

Steps

To enable a closed network:

1. Access the pull down menu for the **Closed Network**.
2. Choose **Enabled** to enable a closed network. Automatic Security Configuration is disabled.



Note: WPS must be disabled before Closed Network can be enabled.

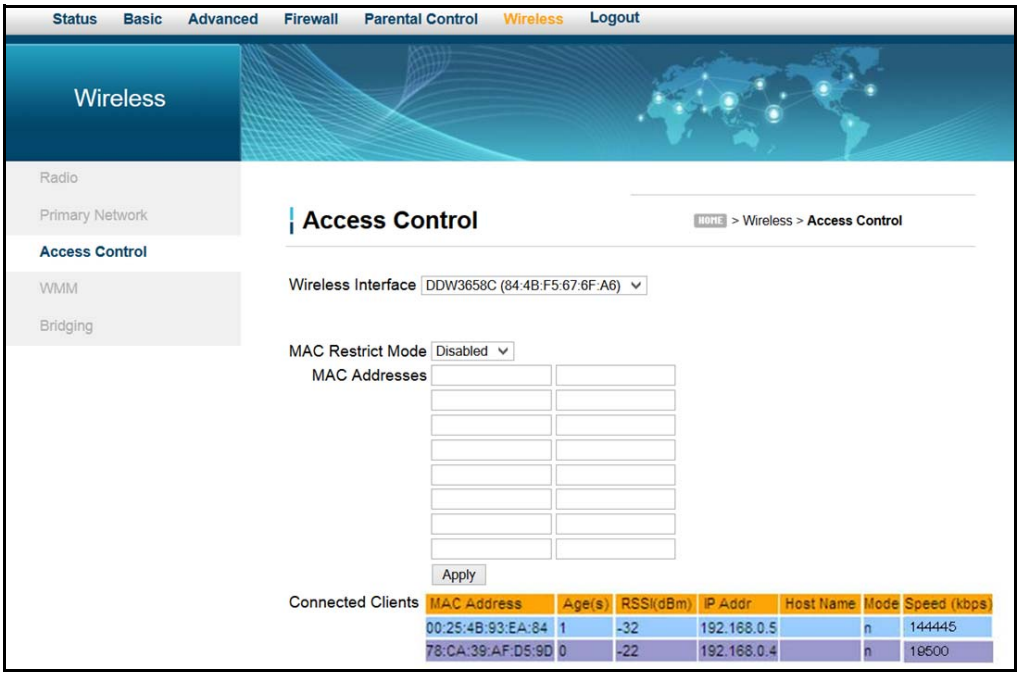
9.3 Using the Access Control Option

Use the **Access Control** option to configure which clients can access your wireless network.

Steps

To configure client access:

1. Click **Wireless** from the main menu.
2. Click **Access Control** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Wireless Interface	Defines the network name (SSID) and MAC address for which you are setting access control parameters.
MAC Restrict Mode	Controls wireless access to your network by MAC address. ♦ **Disabled** turns off MAC restrictions and allows any wireless client to connect to this device. However, if you use other security mechanisms for access to the wireless network, clients must still adhere to those restrictions. ♦ **Allow** creates a list of wireless clients that can connect to the wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields. MAC addresses not on the list, are not allowed access to your wireless network. ♦ **Deny** creates a list of wireless clients that you do not want to have access to your wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields.

Label	Description
MAC Addresses	Defines the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
Apply	Saves changes when clicked.
Connected Clients	Lists wireless clients currently connected listed by MAC address. ♦ **MAC Address** – Displays the MAC addresses entered in the MAC Addresses field (see above). ♦ **Age(s)** – Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data. ♦ **RSSI(dBm)** – Displays the received signal strength from the device to the DDW365. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Understanding Received Signal Strength on page 76 for more information. ♦ **IP Address** – Displays the IP address assigned to this wireless client. ♦ **Host Name** – Displays the host name of the wireless client. ♦ **Mode** – Indicates the applicable 802.11a/b/g/n standard used by the connected client device. ♦ **Speed (kbps)** – Displays the maximum theoretical link speed negotiated between the DDW365 and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible. You can disable WMM if throughput on some client adapters is adversely affected.

9.4 Using the Wi-Fi Multimedia Option

Use the Wi-Fi Multimedia option to configure the quality of service (QoS) to ensure the best service in your wireless networks.

- ❑ Controls WLAN transmission priority on packets transmitted over the wireless network.
- ❑ Wi-Fi Multi-Media Quality of Service (WMM QoS) is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.
- ❑ WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual user and applications. On wireless access points without WMM QoS, all traffic streams are given the same access priority to the wireless network. If a new traffic stream creates a data transmission demand that exceeds the current network capacity, the new traffic stream reduces the throughput of the other traffic streams.

- WMM QoS capability allows you to assign access categories (ACs) to various packet streams. The assigned AC of a packet stream depends on the packet's priority, such as a priority assigned by an application (also referred to as a user priority (UP). An AC may include a common set of enhanced distributed channel access (EDCA) parameters used by QoS to contend for a channel to transmit packets with certain priorities.

  Different ACs can be associated with different power saving parameters. For example, one power saving parameter might be the delivery mechanism used by an access point (AP) to deliver packets to a station (STA) that is operating in a reduced power mode.

- WMM transmit opportunity (TXOP) is assigned to each access point. The bounded time interval during which a station can send as many frames as possible as long as the transmission time does not extend past the maximum duration of the TXOP. If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. Using TXOP reduces the problem of low rate stations gaining too much channel time in the legacy 802.11 DCF MAC. A TXOP time interval of 0 means it is limited to a single MAC service data unit (MSDU) or MAC management protocol data unit (MMPDU).

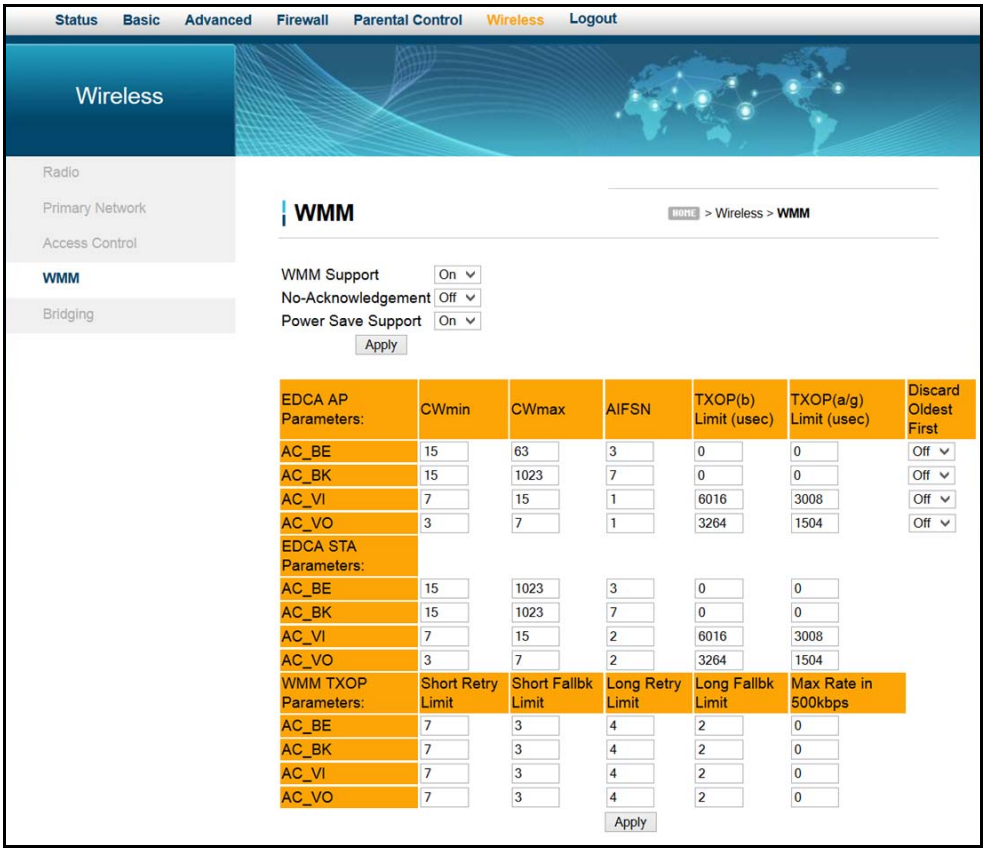
Note

WMM may need to be disabled to avoid throughput impacts to other wireless devices.

Steps

To configure the multimedia wireless option:

1. Click **Wireless** from the main menu.
2. Click **WMM** (Wi-Fi Multimedia**)** from the left side menu. Field descriptions are listed below the screen example.


Status Basic Advanced Firewall Parental Control Wireless Logout
Wireless
Radio
Primary Network
Access Control
WMM
Bridging
WMM
HOME > Wireless > WMM
WMM Support On
No-Acknowledgement Off
Power Save Support On
Apply
EDCA AP Parameters: CWmin CWmax AIFSN TXOP(b) Limit (usec) TXOP(a/g) Limit (usec) Discard Oldest First
AC_BE 15 63 3 0 0 Off
AC_BK 15 1023 7 0 0 Off
AC_VI 7 15 1 6016 3008 Off
AC_VO 3 7 1 3264 1504 Off
EDCA STA Parameters:
AC_BE 15 1023 3 0 0
AC_BK 15 1023 7 0 0
AC_VI 7 15 2 6016 3008
AC_VO 3 7 2 3264 1504
WMM TXOP Parameters: Short Retry Limit Short Fallbk Limit Long Retry Limit Long Fallbk Limit Max Rate in 500kbps
AC_BE 7 3 4 2 0
AC_BK 7 3 4 2 0
AC_VI 7 3 4 2 0
AC_VO 7 3 4 2 0
Apply

Label	Description
WMM Support	Enables (On) or disables (Off) WMM support.
No-Acknowledgement	Enables (On) or disables (Off) acknowledging data frames. In QoS mode, frames to send can have two values: QosAck and QosNoAck. Frames with QosNoAck are not acknowledged, avoiding the retransmission of highly time-critical data.
Power Save Support	Enables (On) or disables (Off) power savings. WMM Power Save increases the efficiency and flexibility of data transmission. The wireless client device can “doze” between packets to save power, while the wireless access point buffers downlink frames. The application chooses the time to wake up and receive data packets to maximize power conservation without sacrificing quality of service.
Apply	Saves changes to the WMM settings above.
EDCA AP Parameters	Allows you to prioritize wireless network traffic. Enhanced Distributed Channel Access – Access Point (EDCA-AP) provides four access categories (ACs): ♦ **AC_BE** – Best Effort, medium throughput and delay. Most traditional IP data is sent to this queue. ♦ **AC_BK** – Background, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (for example, FTP data). ♦ **AC_VI** – Video ♦ **AC_VO** – Voice

CWmin **CWmax** **AIFSN** **TXOP (b) Limit (usec)** **TXOP (a/g) Limit (usec)** **Discard Oldest First**	Sets the time for the following fields: ♦ **CWmin** – Contention window minimum ♦ **CWmax** – Contention window maximum ♦ **AIFS** – Arbitration inter-frame space ♦ **TXOP** – Transmit opportunity ♦ **Discard Oldest First** – Removes oldest frame when set to On.
EDCA STA Parameters	Allows you to prioritize wireless network traffic for receiving terminals. Access categories are: ♦ **AC_BE** – Best Effort, medium throughput and delay. Most traditional IP data is sent to this queue. ♦ **AC_BK** – Background, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (for example, FTP data). ♦ **AC_VI** – Video ♦ **AC_VO** – Voice
WMM TXOP Parameters	WMM TXOP (Wireless Multi-Media Transmit Opportunity Parameters) are used to control the Access Category (AC) for each type of Wireless traffic, including Best Effort (BE), Background (BK), Video (VI), and Voice (VO) traffic categories. Transmission rates will automatically adjust for each category. These settings should be left at their default values. WMM TXOP Access categories are: ♦ **AC_BE** – Best Effort, medium throughput and delay. Most traditional IP data is sent to this queue. ♦ **AC_BK** – Background, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (for example, FTP data). ♦ **AC_VI** – Video ♦ **AC_VO** – Voice
Short Retry Limit **Short Fallbk Limit** **Long Retry Limit** **Long Fallbk Limit** **Max Rate in 500kbps**	Defines how many times the MAC retries to send different types of packets. If the number of retries reach their limit, the frame is discarded.
Apply	Saves all changes.

9.5 Using the Bridging Option

Use the **Bridging** option to configure the DDW365 to act as a wireless network bridge and establish wireless links with other wireless access points. To establish a bridge, you need to know the MAC address of the peer device, that must be in wireless bridging mode as well. The DDW365 can establish up to four wireless links with other wireless access points. When wireless devices are in wireless bridging mode, they form a wireless distribution system that allows computers in one LAN to connect to the computers in the other LAN.

Caution

Avoid bridge loops when you enable bridging devices. Bridge loops cause broadcast traffic to circle the network endlessly. This can degrade throughput and disrupt communications.

Steps

To configure the modem as a bridge:

1. Click **Wireless** from the main menu.
2. Click **Bridging** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
Wireless Bridging	Enables or disables bridging.
Remote Bridges	Defines the MAC addresses of other wireless access points that you want to establish a bridge to and from. These access points must also have bridging enabled.
Apply	Saves all changes.

9.6 Deploying and Troubleshooting the Wireless Network

Use the information in this section to help you understand, deploy, and troubleshoot your wireless environments:

- ❑ Understanding Received Signal Strength on page 76
- ❑ Estimating Wireless Cable Modem to Wireless Client Distances on page 77
- ❑ Selecting a Wireless Channel on page 79

Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the DDW365. This value can significantly impact wireless speeds/performance. It is determined by:

- ❑ Materials (for example, open air, concrete, trees)
- ❑ Distance between wireless clients and the wireless cable modem
- ❑ Wireless capabilities of the client devices

To determine the received signal strength, refer to Using the Access Control Option on page 70 and review the **RSSI** value. A receive signal strength indicator between 0 to -64 dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

Estimating Wireless Cable Modem to Wireless Client Distances

The information in this section helps you to determine how far a wireless cable modem can be placed from wireless client devices. Environmental variances include the capabilities of wireless clients and the types of material through which the wireless signal must pass. When the wireless cable modem and wireless clients reach the distance threshold between each other, network performance degrades.

Steps

To determine wireless cable modem placement:

1. Connect a wireless client to the wireless cable modem. Refer to Connecting Devices to the Network on page 10 if needed.
2. Place the wireless client at around one meter (three feet) away from the wireless cable modem.
3. Obtain the **RSSI** value for the connected client. Refer to Using the Access Control Option on page 70. This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.

Attenuation Considerations at 2.4GHz

Material	Attenuation
Connector/Cable	3.5dB
Free Space	0.24dB / foot
Interior Drywall	3dB to 4dB
Cubicle Wall	2dB to 5dB
Wood Door (Hollow/Solid)	3dB to 4dB
Brick, Concrete Wall (Note 1)	6dB to 18dB
Glass Window (not tinted)	2dB to 3dB
Double Pane Coated Glass	13dB
Bullet Proof Glass	10dB
Steel / Fire Exit Door	13dB to 19dB

Attenuation Considerations at 2.4GHz

Material	Attenuation
Human Body	3dB
Trees (Note 2)	0.15dB / foot
Note 1: Different types of concrete materials are used in different parts of the world and the thickness and coating differ depending on whether it is used in floors, interior walls, or exterior walls.	**Note 2**: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.

5. Use the attenuation value from the materials table above in the following formula:

Formula:

(Transmit Power, **use -30dBm**) **–** (Receiver Sensitivity, **use RSSI value**) **=** Allowable Free Space Loss

Allowable Free Space Loss **÷** Materials Attenuation Value **=** Optimal Distance in Feet Between the Cable Modem and a Wireless Client

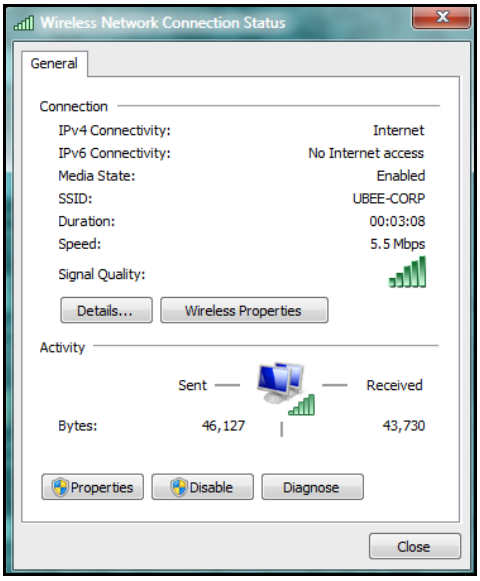
Example:

(-30dBm) **-** (-67dBm) **=** 37dBm (allowable free space loss for a 54Mbps connection)

37dBm **÷**.24db/foot (for open space) **=** 154.16 feet

6. Once you know the optimal feet distance between individual wireless clients and the wireless cable modem, you may resolve and prevent some performance issues.
7. To check the wireless signal strength and speed, use the following steps for a Windows computer connected wirelessly to the wireless cable modem. If the wireless computer is not connected, refer to Connecting a Wireless Device on page 11.
   a. Click the Wireless networking icon in the system tray to display a list of available wireless networks.

   b. Click the Wireless networking icon, click “Open Network and Sharing Center,” then click “Wireless Network Connection.”
   c. Review the speed and signal strength in the Status window.



Selecting a Wireless Channel

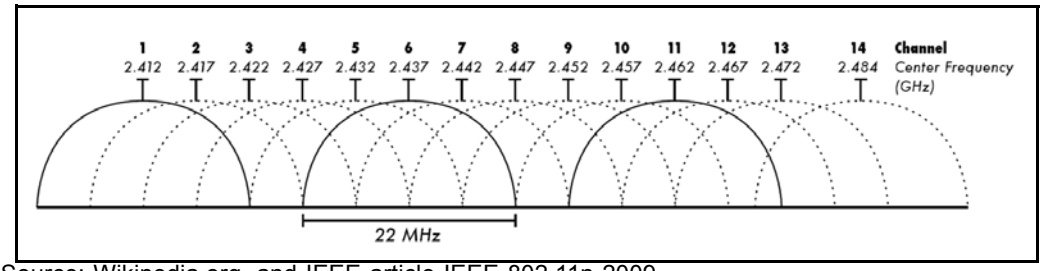
You may need to change the wireless channel on which the DDW365 operates when you are in computing, test, and other environments where several wireless access points may be operating in the 2.4GHz range.

In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel, and so on. This is done by configuring the channel on each wireless access point individually (if you have multiples). If you have control over only one wireless device in an environment where there may be several, you can change the wireless channel on your device to one that is not heavily used.

Note

To change the wireless broadcast channel, refer to Using the Wireless Radio Option on page 63.

The following diagram displays the channels available in the Americas. Each available channel is 22MHz wide. Since channels overlap, it is best to choose channels that have the least overlap (typically 1, 6, and 11 in the Americas, and 1, 5, 9, and 13 in Europe). Overlapping channels can cause wireless network performance issues.



Source: Wikipedia.org, and IEEE article IEEE 802.11n-2009

10 Glossary

This chapter defines terms used in this guide and in the industry.

Broadcast
A packet sent to all devices on a network.

Cable Modem Termination System (CMTS)
Typically located in the cable company's headend, the CMTS is equipment that provides high-speed data services to subscribers, such as cable Internet and Voice over IP (VoIP).

Channel Bonding
A computer networking configuration where two or more network interfaces are combined on a host computer for redundancy or increased throughput. Data is transmitted over these channels as if they are one channel.

Customer Premises Equipment (CPE)
Equipment such as telephones, routers, and modems located at a user's location to enable access to communication services.

Default Gateway
The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

Demilitarized Zone (DMZ)
Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet.

Domain
A subnetwork comprised of a group of clients and servers under the control of one security database.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .org.

Domain Name System (DNS)
An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is actually its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Downstream
A term to describe the direction of data from the network service provider to the customer.

Dynamic Host Configuration Protocol (DHCP)
A protocol that centrally automates the assignment of IP addresses in a network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. For example, when the service provider sets up computer users with a connection to the Internet, an IP address is assigned to each machine. DHCP lets the service provider distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time an IP address is valid for a computer. Lease times can vary.

Ethernet
A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP, HTTP, and FTP.

Firewall
A highly effective method to block unsolicited traffic from outside the connected computers in your gateway and local network.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols. The DDW365 is an example of a gateway.

Headend
A main facility to process and distribute Internet communication signals. Headend may also refer to cable television signals and power line communication facilities.

Internet Protocol (IP)
The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

Internet Service Provider (ISP)
A company that provides individuals and companies access to the Internet and other related services.

Interval Usage Code (IUC)
Interval usage codes define different profiles for upstream burst profiles to use for the data. IUCs are sent to the cable modem from the CMTS to tell the device important characteristics to use for the burst, such as modulation type, preamble length, and so on.

IP Address
In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address. IP sends your IP address to the IP address obtained by looking up the domain name in the URL you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

Local Area Network (LAN)
A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

Maximum Transmission Unit (MTU)
The size in bytes of the largest packet that can be sent or received.

Media Access Control (MAC) Address
A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

Megabits per Second (Mbps)
A unit of measurement for data transmission that represents one million bits per second.

Network Address Translation (NAT)
A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

Packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Ranging
A process in which a cable modem sends a range request at a power of 8 dBmV (very low power). If it does not receive a range response from the CMTS, the cable modem re-transmits the range request at a 3 dB higher power level and continues the process until a range response is received.

Router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol (RIP)
A protocol in which routers periodically exchange information with one another to determine minimum-distance paths between sources and destinations.

Subnet
A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

Subnet Mask
Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

Telnet
A network protocol used on the Internet or a local area network. Provides bi-directional interactive text-oriented communications using a virtual terminal connection.

Terminal Access Controller Access-Control System (TACACS)
A remote authentication protocol used to communicate with an authentication server to determine if the user is allowed to access the network.

Time Division Multiple Access (TDMA)
A method in which cable modems must time-share the upstream channel because there are many cable modems and only one upstream channel frequency.

Transmission Control Protocol (TCP)
A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The basic communication language or set of protocols to communicate over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

Trivial File Transfer Protocol (TFTP)
A file transfer protocol used to transfer automatically configuration or boot files.

Uniform Resource Identifier (URI)
A string of characters used to identify a name or a resource on the Internet.

Uniform Resource Locator (URL)
A uniform resource identifier (URI) that specifies where a known resource is available and how to retrieve it.

Upstream
A term to describe the direction of data from the customer to the network service provider.

Wide Area Network (WAN)
A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.

Wi-Fi Protected Access (WPA)
A security protocol for wireless networks offering improvements over the WEP protocol in the way it handles security keys and the way users are authorized.

Wi-Fi Protected Setup (WPS)
A security protocol for wireless home networks. Created by the Wi-Fi Alliance, this protocol allows home users to easily set up wireless security and add new devices without needing to enter long passwords.

Wired Equivalent Privacy (WEP)
An encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and security for everyday transmissions. To decode data transmissions, all devices on the network must use an identical key.

Wireless Local Area Network (WLAN)
A communications network that uses high frequency radio signals to allow wireless devices to communicate with each other within a limited geographic area.